Use of Biometric Identifying Technology in Schools

NEW YORK STATE OF OPPORTUNITY.

Office of Information Technology Services

TABLE OF CONTENTS

Executive Summary

The New York State Office of Information Technology Services (ITS) was tasked by the state legislature to write a report on the use of Biometric IdentificationTechnology (BIT) in schools. This report consists of a detailed analysis on the 12 tasks provided by the legislature, which include privacy, civil rights, effectiveness, sharing, storage, risk, cost, school use, impact, auditing, disclosure, and legislative impact. Each task is analyzed individually, and the report distinguishes between Facial Recognition Technology (FRT) and Non-FRT BIT, which are the non-facial recognition types of BIT. The report is further broken down into the security versus administrative uses and applications of BIT based on each task being analyzed.

The results from the public survey issued by ITS, as well as from the internal survey of the New York State Education Department (SED), were taken into account when the report was written and are cited throughout. ITS also received feedback from numerous experts and other stakeholders as required by law. Finally, extensive research was conducted regarding this topic and discussed below. Based on this extensive research and outreach, ITS reached the conclusions at the end of the report, which include recommendations about the use of FRT versus the use of other forms of Non-FRT BIT, while acknowledging this technology will continue to evolve and will need to be reevaluated at a future time.

Specifically, based on the research and outreach cited above and discussed below, ITS acknowledges that the risks of the use of FRT in an educational setting may outweigh the benefits, but there are likely lower risks for administrative uses of FRT that individual schools would need to evaluate. The use of digital fingerprinting may also have fewer risks associated with it than with FRT, and there is evidence of the beneficial use of digital fingerprinting for school lunch payments and use of digital educational devices, such as tablets. This may depend on the way the technology is being applied, and individual schools would need to evaluate risks. Lastly, the evidence suggests that handprints, retina and iris patterns, DNA sequencing, and voice and gait recognition is rarely implemented in public, nonpublic, elementary, secondary, and charter schools in New York State. Accordingly, ITS is unable to reach conclusions in this report about these forms of Non-FRT BIT at this time.

Legislative History

On January 25, 2021, the New York State (NYS) Legislature amended State Technology Law (STL) to add Section 106-b (via A.954 of 2021), enacting a moratorium on the purchase or use of Biometric IdentificationTechnology (BIT) in public and nonpublic elementary and secondary schools, including charter schools.

Under this law, the moratorium remained in effect until July 1, 2022, or until such time as the Commissioner of Education (Commissioner) authorizes such purchase or use. Before the Commissioner can authorize such purchase or use of BIT, the Director of ITS, in consultation with the State Education Department (SED), must first issue a report on the use of BIT in the aforementioned educational settings. This report must make recommendations as to what restrictions and guidelines should be enacted to protect individual privacy, civil rights, and civil liberty interests. These recommendations will be made public and presented to the Governor, the Temporary President of the Senate, and the Speaker of the Assembly concerning the 12 topics referenced below (see section D. Overview of Report Structure, *infra*). Accordingly, ITS issues the following report pursuant to STL 106-b, which is designed to help guide SED in future decision-making on this topic. This report should not be considered legal advice to SED or members of the public. ITS acknowledges the ever-changing nature of this technology; it is possible the research conducted and conclusions reached by this report may need to be reevaluated on an ongoing basis.

Introduction

Definitions

Definitions from State Technology Law Section 106-b:

Biometric identifying technology (BIT) – Any tool using an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information.[1]

Biometric information – Any measurable physical, physiological, or behavioral characteristics that are attributable to a person, including but not limited to facial characteristics, fingerprint characteristics, hand characteristics, eye characteristics, vocal characteristics, and any other characteristics that can be used to identify a person including, but not limited to: fingerprints; handprints; retina and iris patterns; DNA sequence; voice; gait; and facial geometry.

Facial recognition/Facial Recognition Technology (FRT) – Any tool using an automated or semi-automated process that assists in uniquely identifying or verifying a person by comparing and analyzing patterns based on the person's face.

Additional definitions and references:

Administrative purposes – Any biometric technology that is utilized for school device authentication (such as a tablet or laptop), used exclusively for access to school services (such as the library or school cafeteria), attendance for students and staff, and fingerprint identification for prospective school employees.

Children – Persons under the age of 13, as utilized for purposes of the Children Online Privacy Protection Act (COPPA); otherwise, use of the term children means an individual below the age of majority.

Education Law Section 2-d – A New York State law that exceeds FERPA (defined below) requirements regarding the privacy and security of student personally identifiable information (PII), as well as certain data regarding teachers and principals. Part 121 of the regulations of the Commissioner of Education, implementing Education Law Section 2-d, became effective in 2019.

Eligible student[2] – As defined in the Family Educational Rights Privacy Act (FERPA), a student who is 18 years of age or older.

Family Educational Rights Privacy Act (FERPA)[3] – A federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

Personally Identifiable Information (PII) – FERPA defines PII as including, but not limited to, a student's name; the name of the student's parent or other family member; a student's address; a student's personal identifiers (such as student number or biometric record) and other information that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

Biometric Record as PII – FERPA defines biometric record as a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting.

School – As used in State Technology Law Section 106-b, includes public or nonpublic, elementary, or secondary schools and charter schools.

---

1 Please note "Biometric Identifying Technology" and "Biometric Identification Technology" will be used interchangeably.

2 Throughout this report, references will be made to "parental consent." This phrase is intended to include the consent provided by eligible students on their own behalf.

3 Family Educational Rights Privacy Act 20 U.S.C. 1232 g and Family Educational Rights Privacy Act Regulations 34 CFR Pt 99

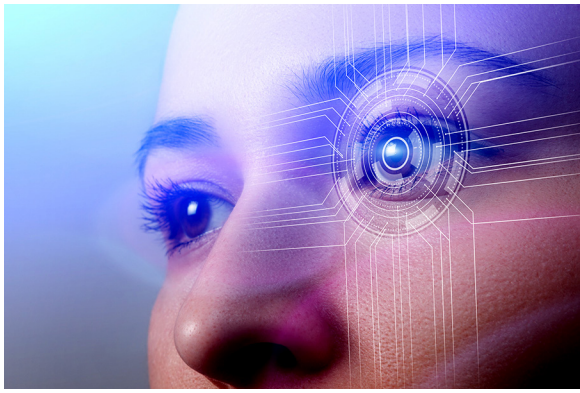
Education Law Section 2-d defines "school" as any (a) public elementary or secondary school, including a charter school; (b) universal pre-kindergarten program authorized pursuant to Education Law Section 3602-e; (c) an approved provider of preschool special education; (d) any other publicly funded pre-kindergarten program; (e) a school serving children in a special act school district as defined in Education Law 4001; (f) an approved private school for the education of students with disabilities; (g) a State-supported school subject to the provisions of Article 85 of the Education Law; or (h) a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.

References to "school" or "schools" under Education Law 2-d do not include nonpublic schools, although they are specifically listed in State Technology Law Section 106-b.

Security purposes – Any BIT that is utilized by school staff, including school safety officers, to identify and authenticate an individual for the purpose of providing access to the school, identifying a weapon, or to be used as evidence of a policy violation to discipline a student or school employee for not following school policies or protocols.

Students – In accordance with State Technology Law Section 106-b, individuals under the age of 18 attending public or nonpublic elementary and secondary schools, including charter schools

Background



The use of BIT has rapidly gained popularity among public and private institutions in the U.S. within the past decade.[4] The market for biometric data systems is expected to grow from $33 billion in 2019 to $65 billion by 2024.[5] BIT automatically identifies individuals by matching real-time biometric information to electronically stored biometric information. For example, FRT allows many iPhone users to access their phones by automatically identifying individuals by matching two or more faces from digital images.[6] The various facial features of an individual are measured and then compared with features of other known faces through an algorithm to find a match.

There are two types of BIT algorithms: "one-to-one" and "one-to-many."[7] "One-to-one" matching is when an algorithm verifies an individual's identity by comparing the biometric information presented with the biometric information of an individual. A familiar example of this would be using facial identification to unlock a phone, which compares the face presented upon attempting to log in with the stored data of a known face. "One-to-many" matching compares an unknown individual's biometric information to an entire database of stored biometric information of many faces in an attempt to find a match. Some police agencies use one-to-many algorithms when comparing an individual's facial characteristics with those in a database to identify individual.

---

4 Rachel German and K. Suzanne Barber, Current Biometric Adoption and Trends, U. TX Ctr. Idty. UT CID Report #18-02 (9/2017) https://identity.utexas.edu/sites/default/files/2020-09/Current%20Biometric%20Adoption%2and%20Trends.pdf (last accessed 3/17/2023)

5 Identity Management Institute, Biometric Data Breach Security Threats, (2/25/2020), Identity Mgmnt. Inst., https:/identitymanagementinstitute.org/biometric-data-breach-security-threats/ (Last Accessed 3/6/2023

6 EU Agency for Fundamental Rights, *Facial Recognition Technology: Fundamental rights considerations in the context of law enforcement*, FRA Focus (11/21/2019), https://fra.europa.eu/en/publication/2019/facial-recognition technology-fundamental-rights-considerations-context-law (Last Accessed 3/6/2023)

7 Apple Inc, *About Face ID Advanced Technology*, Apple Inc (4/27/2022) https://support.apple.com/en-us/HT208108 (last accessed 3/17/2023)

7 Lindsey Barrett, *Ban Facial Recognition Technologies for Children--And for everyone else*, 26 B.U. J. Sci. & Tech. Law 223, 232-233 (8/22/2020) https://www.bu.edu/jostl/files/2020/08/1-Barrett.pdf (Last Accessed 3/6/2023)

Similarly, there are two types of errors that can occur when utilizing both types of BIT algorithms: false positives and false negatives. False positives occur when the person is erroneously matched with stored BIT data of another individual, and false negatives occur when the algorithm erroneously rejects the person whose biometric information was presented.[8] False negatives could lock someone out of their mobile device or building, and false positives could lead to security breaches. False positives could also lead to law enforcement misidentifying an individual as the suspect of a crime[9].

Schools can utilize BIT in several different ways. BIT that utilizes facial geometry, fingerprints, handprints, retina and iris patterns, DNA sequence, voice, or gait would allow schools to verify student attendance, allow students and staff to access services and certain parts of school buildings with restricted access, verify student identities, and allow access to devices such as laptops and iPads.[10] BIT that utilizes FRT could allow schools to track students throughout the day, identify individuals that attempt to enter the school, and flag other unwanted and unknown individuals that attempt to enter the school, such as individuals subject to custody and restraining orders. Although these various forms and uses of BIT are technically possible, they are not currently authorized for use in NYS schools.[11] Though some forms of BIT, such as fingerprinting, have been commonly used in schools in recent years (prior to the passage of STL Section 106-b), there is no information documenting the use of other forms of BIT listed in STL Section 106-b.[12]

This report will discuss the risks and benefits of FRT and other BIT, as well as circumstances in which the technology may be appropriate. However, each specific technology and application of it is different, and schools must balance not just the risks and benefits of the technology itself, but also the costs of the technology relative to overall school funding, the age and demographics of students, and the goals of the use of the technology and the systems or processes it supports.

Notably, as one-to-one facial recognition processes are used for device security (such as the ability to unlock a phone, tablet, or computer using FRT), schools may need to carefully balance risks of one-to-one FRT on devices against the benefits of using the related technology solutions, even if they choose to more stringently limit one-to-many FRT technologies. The evolution of this technology may also result in further research to accurately evaluate its efficacy in school settings.[13] While intended to be informative, this report should not be considered a final resolution to whether this technology should be used in schools.

ITS conducted a survey in 2022 on the use of FRT and other forms of BIT in school settings. ITS received roughly 1,000 responses to this survey, in which questions were asked of parents, school staff, vendors, and other school personnel. Questions included, but were not limited to, the concerns people may have with the technology, its expected efficacy, and whether the risks associated with the technology outweighed the benefits. The responses in this survey were overwhelmingly against the use of FRT and other forms of BIT in school settings. A copy of the survey and responses is

---

8 See Barrett, pp. 232-233

9 See id.

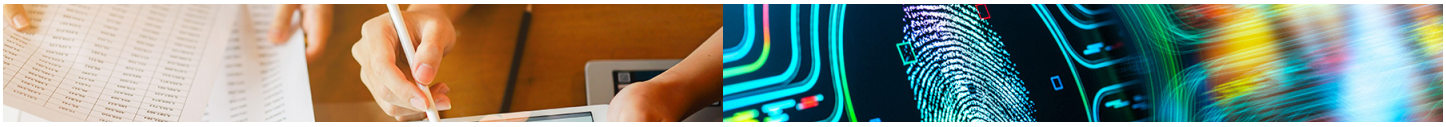
10 Marcela Hernandez-de-Menendez, Biometric Applications in Education, 48 Int'l J. Interactive Design Mfg. 365 (IJIDeM) (2021) https://link.springer.com/article/10.1007/s12008-021-00760-6, https://link.springer.com/content pdf/10.1007/s12008-021-00760-6.pdf (Last Accessed 3/6/2023)

11 Id.; NYS Tech. L §106-b

12 To date, the use of DNA sequencing to identify individuals has been generally regarded as too slow for widespread use and is usually restricted to law enforcement. Lenildo Morais, *Biometric Data: Increased Security and Risks*, www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks (last accessed March 6, 2023).

13 Nestor Maslej, Facial Recognition Technology (FRT) in 2022: What the Data Tells Us, AI Index and Stanford Institute for Human-Centered Artificial Intelligence Standing Committee on Access to Information, Privacy and Ethics (6/9/2022) https://www.ourcommons.ca/Content/Committee/441/ETHI/Brief/BR11882158/br-external MaslejNestor-e.pdf

found attached in Exhibit A.[14] Regardless of what, if any, technologies a school wishes to use, the survey response indicates that schools should consider working closely with stakeholders to ensure that any implementation is clearly understood for the best chance of success.



Methodology

ITS conducted a comprehensive review of literature discussing the implications of FRT and non-FRT BIT. The issues and tasks presented by the legislature are the subject of numerous articles ITS reviewed. ITS' research methodology maintained an objective standpoint and included reviews of arguments and sources that reflect the entire spectrum of opinion on the use of BIT in schools.

Pursuant to STL 106-b, ITS conducted a survey on the use of biometrics in school settings.[15] This study was conducted to receive feedback from teachers, school administrators, parents, students, school staff, school security personnel, vendors, law enforcement, civil rights groups, and any other interested individual or organization. Numerous outreach methods were used to make the survey available to the general public and any interested parties. Outreach was conducted on social media, and a formal press release was posted on ITS' website. Additionally, the survey was sent to every single school administrator in NYS from a list provided by SED. The survey was also sent to numerous other interested parties, such as vendors and civil rights groups. The survey was opened on June 23, 2022, and closed on Oct. 28, 2022 at 5 p.m.

ITS also made available a public email inbox for any individual or organization that wished to make comments on the use of biometrics in schools. ITS received general feedback in this inbox from numerous individuals and organizations about the use of biometrics in schools. Organizations included vendors and civil rights groups.

Pursuant to STL 106-b, ITS conducted a virtual public hearing on Oct. 20, 2022 at 5:30 p.m. on the use of biometrics in school settings. ITS sent notice of the public hearing to numerous interest groups and the general public on Oct. 11, 2022. Five different individuals testified at the public hearing in either their individual capacity or as representatives of a larger organization, such as a vendor or civil rights group. Individual written testimony was also submitted by individuals and organizations prior to the hearing. Sixty-seven non-participants attended the hearing, and a recording of the hearing was made publicly available on ITS' website.

Pursuant to STL 106-b, ITS sought feedback and assistance from the NYS Department of Criminal Justice Services (DCJS), NYS Police (NYSP), NYS Department of Corrections and Community Supervision (DOCCS), State University of New York (SUNY), City University of New York (CUNY), as well as numerous other internal and external individual experts in data and student privacy issues, and civil liberties and civil rights.

Types of Biometric Identifying Technology

BIT is constantly developing, and new methods of identification may become viable in the not-so-distant future. However, because these were enumerated in the definition of "biometric information" in the legislation, the types of BIT addressed in this report are limited to the following:

Facial recognition technology (FRT)
Fingerprint and handprint recognition technology
Voice recognition technology
Iris and retina recognition technology
DNA sequencing technology
Gait recognition technology

14 See Exhibit A.

15 See Exhibit A

Overview of Report Structure

As tasked by the legislature in STL Section 106-b, this report will consider, evaluate, and present recommendations in the report concerning:

1. *Privacy Implications* – "The privacy implications of collecting, storing, and/or sharing biometric information of students, teachers, school personnel and the general public entering a school or school grounds."

2. *Impact on Civil Rights* – "The potential impact of the use of BIT on student civil liberties and student civil rights, including the risks and implications of the technology resulting in false facial identifications, and whether the risks of false facial identifications differ for different subgroups of individuals based on race, national origin, gender, age and other factors, as well as any other reasonable accuracy concerns with respect to technology."

3. *Effectiveness* – "Whether, and under what circumstances, such technology may be used for school security and the effectiveness of such technology to protect students and school personnel."

4. *Sharing* – "Whether, and under what circumstances and in what manner, information collected may be used by schools and shared with students, parents, or guardians, outside agencies including law enforcement agencies, individuals, litigants, the courts, and any other third parties."

5. *Storage* – "The length of time biometric information may be retained and whether, and in what manner, such information may be required to be permanently destroyed."

6. *Risk of Breach*[16] – "The risk of an unauthorized breach of biometric information and appropriate consequences therefore."

7. *Cost* – "Expected maintenance costs resulting from the storage and use of facial recognition images and other biometric information, including the cost of appropriately securing sensitive data, performing required updates to protect against an unauthorized breach of data, and potential costs associated with an unauthorized breach of data."

8. *Analysis of Other Schools* – "Analysis of other schools and organizations, if any, that have implemented facial recognition technology and other BIT programs."

9. *Impact of Using Existing Databases* – "The appropriateness and potential implications of using any existing databases, including but not limited to local law enforcement databases, as part of BIT."

10. *Auditing* – "Whether, and in what manner, such BIT should be assessed and audited, including but not limited to vendor datasets, adherence to appropriate standards of algorithmic fairness, accuracy, and other performance metrics, including with respect to subgroups of persons based on race, national origin, gender, and age."

11. *Disclosure* – "Whether and in what manner the use of such technology should be disclosed by signs and the like in such schools, as well as communicated to parents, guardians, students, and district residents."

12. *Legislative Impact* - "Existing legislation, including but not limited to Section 2-d of the Education Law, that may be implicated by or in conflict with biometric technology to ensure the maintenance of records related to the use of such technology, protect the privacy interest of data subjects, and avoid any breaches of data."

16 The term "breach" is used in STL Section 106-b, and therefore we will use it throughout this report. However, a "breach" generally refers to outside actors accessing data without authorization. The more general term "unauthorized disclosure" includes both breaches and instances of accidental disclosure. When "breaches" are referred to in this report, they should be understood to include all instances of unauthorized disclosure.

Because the use of FRT in school settings may have unique impacts that use of other BIT does not necessarily have, this report will separately discuss FRT and other, non-FRT BIT in educational settings. However, there are circumstances and applications wherein concerns may overlap. These instances will be noted.

Finally, this report will compare different applications of BIT technology, including security-related purposes and administrative-related purposes. While this report recognizes that there may be overlapping concerns, we hope that by addressing types of use separately, schools may be better able to balance the risks and benefits of using various technologies, thereby allowing schools to craft policies and procedures to further their educational needs in accordance with the use and purpose authorized by the Commissioner and data privacy laws. "Security purposes" and "administrative purposes" are defined in Section A – Definitions.

Analysis

Privacy Implications

General Considerations

FERPA, COPPA, Education Law Section 2-d, 8 NYCRR Part 121

Student PII – which includes biometric data – is generally protected from disclosure in accordance with FERPA and NYS Education Law Section 2-d (Section 2-d). Additionally, Section 2-d (4) (a) requires SED to promote the least intrusive data collection policies practicable that advance the goals of improving academic achievement, empowering parents with information, and advancing efficient and effective school operations while minimizing the collection and transmission of PII. Section 121.2 (b) of Part 121 of the regulations of the Commissioner of Education (Part 121) further requires that all schools take steps to minimize the "collection, processing and transmission of PII."

Therefore, schools should collect and store only the minimum amount of personal information necessary to effectively perform the educational task associated with that collection and should delete or destroy the personal information once the task is completed, in compliance with appropriately implemented record retention and data destruction policies.[17]

Additionally, Section 2-d (5) requires schools to enter into a contract or other written agreement, which must include certain minimum provisions to ensure the protection of student data when sharing with third-party contractors. Section 2-d (6) also requires third-party contractors to notify schools in the event of a data breach. A school that is notified is required to report the breach to the Chief Privacy Officer of SED, who may then investigate and potentially impose penalties.

New York has no common law right to privacy,[18] but FERPA[19] requires that schools receive prior written consent from the parent or eligible student before disclosing personally identifiable information (PII) from students' education records to a third-party. However, FERPA contains several exceptions to this requirement. For example, if a school has implemented a directory policy in accordance with the regulations implementing FERPA, the school may release certain information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed.[20] Also, schools may release PII from students' education records to third-party contractors under FERPA's "school official" provision if the school determines that the vendor qualifies as a "school official" with a "legitimate educational interest."[21] FERPA's regulations permit schools to share PII with contractors, consultants, volunteers, or other

17 If the use of BIT is authorized by the Commissioner after the issuance of this report, biometric data will be encompassed in schools' requirements to ensure they have a policy on data security and privacy in accordance with NYS Ed Law §2-d (5).

18 *Ava v. NYP Holdings, Inc.*, 20 Misc. 3d 1108(A) (Sup. Ct. NY County 2008)

19 *Family Educational Rights Privacy Act Regulations* 34 CFR Pt 99

20 *Family Educational Rights Privacy Act Regulations* 34 CFR §§ 99.3, 99.37

21 *Family Educational Rights Privacy Act* 20 USCA 1232g (b)(1)(A)

third parties, designated as "school officials," who are performing institutional services or functions, provided that the outside entity: 1) performs an institutional service or function for which the school would otherwise use employees; 2) is under the direct control of the school with respect to the use and maintenance of the education records; 3) uses the PII only for the purpose for which the disclosure was made; and 4) meets the criteria specified in the school's annual notification of FERPA rights for being a "school official" with a legitimate educational interest in the education records. [22]

The Children's Online Privacy Protection Act (COPPA)[23] is a federal law that governs private companies that collect children's personal information and adds yet another layer, albeit limited, of data privacy protection for some students. Under COPPA, companies are required to obtain parents' consent before collecting the personal information of children under thirteen years old. However, the Federal Trade Commission (FTC), which oversees COPPA, has issued guidance stating that schools "may act as the parent's agent and can consent under COPPA to the collection of kids' information on the parent's behalf." The guidance does clarify that this is limited to an educational context and not for commercial purposes.[24]

Although FERPA and COPPA allow PII to be shared with outside entities, Section 2-d and its implementing regulations, Part 121, require additional protections for the privacy and security of student PII and the annual professional performance review (APPR) information for teachers and principals in New York State. Section 2-d requires schools to adopt a parents' bill of rights for data privacy and security, as well as publish it on their website. When a school shares student data with a third-party contractor, the parties must enter into a data sharing agreement, and information on that agreement must be shared with parents on the school's website.[25,26] Also, Section 2-d and Part 121 require schools to adopt and conform with the National Institute of Standards Technology (NIST) Cybersecurity Framework to protect PII and teacher and principal APPR data.[27]

Fourth Amendment Considerations

An additional privacy implication for school collection and storing of biometric facial information of staff, students, or members of the public for security purposes is raised under the Fourth Amendment to the U.S. Constitution. The Fourth Amendment protects the right of individuals to be secure in their persons from unreasonable searches and seizures by the government. In its *Katz v. United States* decision, the U.S. Supreme Court specified that an individual's protections include any areas in which they have a "reasonable expectation of privacy."[28] While limits to government collection of citizen's BIT have not yet been established, the *Katz* test is typically applied to cases in which technological advancements create search-related privacy concerns.[29]

The Fourth Amendment may provide some protection from FRT privacy intrusion, depending on the way FRT is used.[30] There are constitutional gaps in Fourth Amendment protection that could be addressed by legislative action.[31] For exam-

---

22 *Family Educational Rights Privacy Act Regulations* 34 CFR 99.31

23 *Children's Online Privacy Protection Act* 15 USCA Section 6501

24 Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions: Section N* https://www.ftc.gov business-guidance/resources/complying-coppa-frequently-asked-questions#N.%20COPPA%20AND%2 SCHOOLS(Last accessed 3/17/2023)

25 NY Educ. L. Section 2-d and 8 NYCRR Pt 121

26 *Blueprint for an AI Bill of Rights: Making automated systems work for the american people*, White House Off. Sci. Tech. Pol'y. (10/2022) https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights pdf (Last Accessed 3/6/2023) Blueprint for an AI Bill of Rights is a white paper published by the White House Office of Science and Technology Policy; is non-binding and does not constitute U.S. government policy.

27 NYS Educ. L 2-d(5); 8 NYCRR 121.5

28 Katz v US, 389 US 347 [1967]).

29 Tokson, Mathew (2016). "KNOWLEDGE AND FOURTH AMENDMENT PRIVACY". Nw. Univ. L. R. (12/2016) https://northwesternlawreview.org/issues/knowledge-and-fourth-amendment-privacy/ (Last Accessed 3/6/2023)

30 Andrew Ferguson, *Facial Recognition and the Fourth Amendment*, 105 Minn. L. R. 1105 (2021), https:/ digitalcommons.wcl.american.edu/facsch_lawrev/742 (Last Accessed 3/6/2023

31 Id.

ple, if FRT is used for identity verification at established points of entry at a public school, the Supreme Court would likely view this use differently under the Fourth Amendment than FRT that is used for law enforcement and investigatory purposes because a false negative identification could bar a student from accessing their education.[32] Additionally, ongoing surveillance, tracking, and aggregation of locational data could rise to the level of a search under the Fourth Amendment, as could the comparison of facial images to a large-scale police database if schools were authorized to use such databases.[33] Given the qualitative and quantitative differences between regular surveillance and using security cameras and networked systems of identification using FRT software, courts could view FRT differently than regular surveillance and security cameras.[34]

While safety concerns could legitimize the use of FRT for school visitors, it may not always be appropriate for use on students. For example, public schools are required to have a reasonable suspicion of improper behavior by a particular student before they conduct a search of that student,[35] but the Supreme Court made clear in *Carpenter v. United States* that the Fourth Amendment does not apply to conventional surveillance techniques, such as security cameras.[36] However, if a school were to use FRT, depending upon the purpose of its use, there could be a reasonable expectation of privacy in the mathematical data taken from the biometric measurements of one's face, due to the anti-equivalence of security cameras and cameras using FRT software.[37]

Of particular concern to privacy advocacy groups is the phenomenon of "mission creep." Mission creep happens when a technology is deployed for a particular purpose, but then slowly starts to be used for other purposes. An example provided by the University of Michigan's Gerald R. Ford School of Public Policy's report, "Cameras in the Classroom," involved CCTV cameras in the UK. Originally installed for security purposes, the cameras were soon used to monitor student behavior, normalizing a constant surveillance state in schools.[38]

There is also the potential for additional privacy risks if FRT were to be used on children.[39] According to some studies, the use of FRT on children could have a negative effect on intellectual development and behavior, and this could result in early exposure to the criminal justice system.[40]

32 Id.

33 Id.

34 Id.

35 Safford Unif. Sch. Dist. #1 v Redding, 557 US 364 (2009)

36 Carpenter v. US, 138 S. Ct. 2206 (2018) ; See Facial Recognition and the Fourth Amendment.pdf

37 See Facial Recognition and the Fourth Amendment.pdf

38 Claire Galligan et al, *Cameras in the Classroom: Facial recognition technology in schools*, University of Michigan (8/25/2020) https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition technology-schools (last accessed 3/17/2023)

39 Barrett

40 Barrett

Cybersecurity Standards

According to NIST, a federal agency that develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public (including educational agencies), a biometric data breach could have serious implications on individuals whose data is compromised. These harms could include intangible harms, such as embarrassment and stigma, as well as tangible harms, such as discrimination, physical harm, or economic harm.[41]

While there is no federal or state law requiring specific biometric standards, NIST has developed and approved voluntary standards for the use of biometric data. The current version of these standards is ANSI/NIST-ITL 1-2011.[42] These standards continue to evolve, and as of the date of this writing, NIST is working on promulgating standards for the federal government's use of biometric technology that respect information privacy and other individual rights.[43]

Data privacy should be considered throughout the lifecycle of any BIT data system or program, including, but not limited to a strong data governance system, strong controls over the data, and a data minimization policy. These privacy tenets are included in Education Law Section 2-d.[44]

---

41 *See generally:* NIST, *Getting Started with the NIST Cybersecurity Framework*, NIST Sp. Pub. 1271 (8/2021) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf (last accessed 3/17/2023)

42 More information on the NIST standards can be found at: NIST, *Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011*, NIST Special Publication 500-290 Edition 3 (8/22/2016) https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist itl-1-1

43 See generally: *Federal Government Approaches To Issuing Biometric Ids: Part II: Hearing before the US H Comm. Oversight Gov't Reform, S. Comm. Gov't. Ops.* (6/19/2013), (Statement of Dir. Charles H. Romine of the NIST IT Lab.) https://www.nist.gov/speech-testimony/standards-biometric-technologies#:~:text=Starting%20in%2 1986%2C%20

NIST%20has%20developed%20and%20approved,Interchange%20of%20Fingerprint%2C%20Facial%20%26%2 Other%20Biometric%20Information. and Educ. L. §2-d

44 United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (Last Accessed 3/6/2023)

Administrative vs. Security Uses of FRT

Whether used for administrative or security purposes, FRT allows for individuals to be automatically identified by matching two or more faces from digital images or facial geometry.[45] During the facial recognition process, a camera will locate a face and analyze it via facial recognition software. Measurements of the face are taken and then converted into unique mathematical data. This data is then compared either to a known, digitally stored image of a face in a one-to-one process or to a database of the mathematical data of other facial images in a one-to-many process, in an attempt to find a match. The privacy implications of collecting, storing, and sharing the biometric facial data of students, school staff, and the pub-lic stem from the uniqueness of one's facial biometric information. One's face is not something that can be well hidden or encrypted, and one's biometric facial data can easily be detected from afar by FRT without the subject's knowledge. Compromised biometric facial data could result in the disclosure of physical characteristics that cannot be replaced, as compared to a credit card or social security number, which could be changed if necessary.[46]

Authorizing the use of only one-to-one processes could reduce privacy concerns, since matching live biometric data of the user to stored biometric data is all that is needed to identify the individual.[47] Because the individual is present in a one-to-one process, there is greater control over the use of the biometric data, as well as increased security because there is no need to have additional identifying information attached to the stored biometric data.[48] Also, FRT data on a one-to-one FRT enabled device is stored locally on the device rather than in the cloud[49], which enables the user to control whether their face is used on the device, disabled or permanently deleted from a device.[50] One-to-many processes, often used in security, could present more privacy concerns than one-to-one due to the fact that these processes usually require more biometric data and could be prone to more errors.[51] In addition, subjects may not be aware that their biometric data is being used in many one-to-many FRT systems, especially those used for security and law-enforcement applications.[52]

45 See Barrett

46 Lenildo Morais,*Biometric Data: Increased Security and Risks,* Sec. Mag. (May 6, 2020) https://www.securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks (Last Accessed 3/6/2023).

47 Information and Privacy Commissioner of Ontario, *Privacy by Design Solutions for Biometric One-to-Many Identification Systems*, Info. Privacy Comm'r Ontario (6/2014) https://www.ipc.on.ca/wp-content/uploads/2014/06 pbd-solutions-biometric.pdf (Last Accessed 3/6/2023)

48 Id.

49 *See generally:* Germain, T. (2017, September 11). *Why Facial Recognition Technology Could be the Best Way to Unlock Your Phone*. Retrieved 2023, from https://www.consumerreports.org/smartphones/why-facial-recognition-could-be-the-best-way-to-unlock-your-next-phone/

50 See generally: Use Facial recognition security on a Galaxy phone or tablet (samsung.com); and see: About Face ID advanced technology - Apple Support

51 Id.

52 Clare Garvie et al, *The Perpetual Line-Up: Unregulated police face recognition in america*, Georgetown Law Center on Privacy and Technology (10/18/2016) https://www.law.georgetown.edu/privacy-technology-center publications/a-forensic-without-the-science-face-recognition-in-u-s-criminal-investigations/#:~:text=The%2 Perpetual%20Line-Up%3A%20Unregulated%20Police%20Face%20Recognition%20in,is%20used%20by%2 police%20in%20the%20United%20States. (last accessed 3/17/2023)

Notably, as one-to-one facial recognition processes are used for device security (such as the ability to unlock a phone or computer using FRT), schools may need to carefully balance risks of one-to-one FRT on a device level against the benefits of using the related technology solutions, even if they choose to more stringently limit one-to-many FRT technologies.

Administrative vs. Security Uses of Non-FRT BIT

The privacy implications for non-FRT BIT, whether used for either security or administrative purposes, could be less severe, especially if the BIT is used in a one-to-one process instead of one-to-many.[53] Unlike FRT, a technology which can easily be used on an individual without their knowledge or consent, the possibility of capturing BIT such as fingerprints, handprints, retina/iris patterns, and DNA sequence without the individual's knowledge is less likely. This type of BIT could be used on a consensual, opt-in basis when students use a product.[54] Similar to FRT, voice and gait identifiers could be used without subjects' consent or even knowledge; however, based on a survey conducted by SED for this report, of 212 respondents, no schools reported that they are using these forms of BIT.[55]

Schools using non-FRT BIT data for either security or administrative purposes would be subject to the same requirements under Section 2-d, Part 121, and FERPA as FRT because biometric data is PII and is part of a student's education record maintained by the school. As discussed in Section 1(a)(i), under FERPA, schools must get written consent from parents and eligible students to disclose personally identifiable biometric data from education records to a third-party unless the release falls under an appropriate exception.[56]

As noted above, the use of non-FRT BIT as a security feature (such as using a fingerprint to unlock a device) may result in schools needing to craft policies balancing uses of non-FRT BIT on a device level, even if they choose to craft more restrictive policies on broader uses of BIT overall.

Impact on Civil Rights

General Considerations

FRT and non-FRT BIT systems, at their core, automate decision-making processes that have traditionally been performed by humans. Given the potentially higher rate of false positives for people of color, non-binary and transgender people, women, the elderly, and children, the use of FRT in schools for security purposes may implicate civil rights laws.[57] Title VI of the Civil Rights Act of 1964[58] prohibits discrimination in federally funded programs or activities on the basis of race or national origin, and the Age Discrimination Act of 1975[59] prohibits discrimination on the basis of age in federally funded programs. Any school that receives federal funding and installs FRT for security purposes could be subject to civil penalties under these laws and others if the FRT in use is found to have a disparate impact on protected groups. In addition, NYS Executive Law Section 291 establishes the civil right to access education without discrimination on the basis of age,

---

53 Privacy by Design Solutions for Biometric One-to-Many Identification Systems.pdf

54 It is important to remember that the use of these technologies does not require consent in accordance with FERPA, wherein a vendor may be determined to be a "school official" and may therefore be allowed access to PII without consent, and in accordance with COPPA, which has guidance authorizing schools to act "en loco parentis" and contract with vendors without obtaining parental consent.

55 Exhibit B, Office of Information Technology Services and NYS Education Department, *Educational Agency Use of Biometrics Study*, or See Exhibit B/Appendix/Attachment # *Educational Agency Use of Biometrics Study* of the Name of actual Report here

56 United States Department of Education, *An Eligible Student Guide to the Family Educational Rights and Privacy Act (FERPA) SPPO-23-01*, US. Ed. Dept. (3/8/2023), https://studentprivacy.ed.gov/sites/default/files/resource_document file/An%20Eligible%20Student%20Guide%20to%20FERPA_0.pdf (last accessed 3/6/2023); United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https://studentprivacy ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (last accessed 3/6/2023)

57 Id.

58 42 U.S.C. Section 2000D ET SEQ.

59 42 U.S.C. 6101-6107

race, creed, color, national origin, sexual orientation, gender identity or expression, military status, sex, marital status, or disability. Noting the potential for disparate impact, the White House's Office of Science and Technology Policy released its "Blueprint for an AI Bill of Rights" in the fall of 2022, wherein it states, "[c]ontinuous surveillance and monitoring should not be used in education, work, housing, or in other contexts where the use of such surveillance technologies is likely to limit rights, opportunities, or access."[60] Even if these technologies are rendered more technically accurate, "it can be argued that sorting students into socially constructed racialized and/or gendered categories remains a discriminatory practice – conflating biological characteristics with social attributes."[61]

Administrative vs. Security Uses of FRT

Although evidence suggests that false facial identifications occur at a higher rate for people of color[62], non-binary and transgender people, women[63], the elderly, and children, [62] it should be noted that the Department of Homeland Security conducted a study in 2019, which concluded that the accuracy of the technology is improving.[63] For example, FRT can work well across demographic groups if no masks are worn.[64] However, in one example, the American Civil Liberties Union's (ACLU) demonstrated the potential for harmful disparate impacts in 2018 when it experimented with Amazon's FRT system, Rekognition.[65] The ACLU used Rekognition to build an FRT database and search tool using 25,000 publicly available arrest photos, then searched that database using public photos of House and Senate representatives. Rekognition falsely matched 28 members of congress to mugshots, identifying them as other people who have been arrested for a crime.[66] The members of Congress who were falsely matched were Republicans and Democrats, men and woman, and varied in age. Nearly 40 percent of Rekognition's false matches during the ACLU's test were people of color, even though people of color only make up only 20 percent of Congress.[66] Amazon has since issued a moratorium on selling Rekognition for law enforcement purposes and has begun alerting customers of the limitations of the product.[67] However, Amazon has also recently been accused of failing to notify Amazon Go customers of Amazon's use of biometric technology in Amazon Go stores.[68]

---

60 *Blueprint for an AI Bill of Rights: Making automated systems work for the american people*, White House Off. Sci. Tech. Pol'y. (10/2022) https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights pdf (Last Accessed 3/6/2023) Blueprint for an AI Bill of Rights is a white paper published by the White Office of Science and Technology Policy; is non-binding and does not constitute U.S. government policy.

61 Mark Andrejevic and Neil Selwin, *Facial Recognition Technology In Schools: Critical Questions And Concerns* Learning, Media and Technology v45, Issue 2 pp 115-238 (11/5/2019) https://www.tandfonline.com/doi/full/10./17439884.2020.1686014 (last accessed 3/17/2023)

62 According to the New York State Education Department's "Education at a Glance" data site, 56.8% of school students were people of color and 48.7% of public school students were female in 2022. See https://data nysed.gov/ (last accessed 1/17/2023). Please note: although NYS began collecting non-binary gender information for students in 2022, that information was not yet available at the time of publication.; Barrett;

63 Jacob A. Hasselgren, *A Scenario Evaluation of High-Throughput Face Biometric Systems: Select Results from the 2019 Department of Homeland Security Biometric Technology Rally*, U.S. Dept. Homeland Sec., Sci. Tech. Dir., Biometric and Identity Tech. Ctr. (8/2020) https://www.dhs.gov/sites/default/files/publications/2021_st-01_2019sel ctrallyresultstip20201104_revised_3046.pdf (Last Accessed 3/6/2023)

64 Id.

65 Jacob Snow, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, A.C.L.U. (7/26/2018) https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28 (Last Accessed 3/6/2023)

66 Id.

67 See Jeffrey Dastin and Paresh Dave, Amazon to warn customers on limitations of its AI, Reuters (11/30/2022) https://www.reuters.com/technology/amazon-warn-customers-limitations-its-ai-2022-11-30/

68 Kevin Collier, Amazon sued for not telling New York store customers about tracking biometrics, NBC

If authorized, schools may need to exercise caution with the use of FRT to ensure that vulnerable populations are not disproportionately impacted, such as people of color, non-binary and transgender people, women, the elderly, and children.[69] There could be additional effects for children as discussed in section 2a. Students and children especially might be at higher risk of their pictures being utilized in facial recognition databases without their parent's consent because, as discussed in Section 1.a.i, both COPPA and FERPA allow schools to enter into contracts with third party vendors, sharing student data without parent consent. Additionally, the use of FRT could have a negative effect on student intellectual development and behavior, as this type of surveillance has been shown to erode student anonymity and impact how students behave and think of themselves, potentially becoming detrimental to the social and emotional well being of students in educational settings.[70]

The use of FRT for security purposes could also result in students having an early, negative exposure to the criminal justice system. According to Lindsey Barrett, Staff Attorney and Teaching Fellow at the Communications and Technology Law Clinic at Georgetown University Law Center and author of "Ban Facial Recognition Technologies for Children – and for Everyone Else," if student data is shared to a law enforcement database that could be searched by a police officer at any time, this could result in errors in law enforcement investigations that have consequences on students' safety, freedom, and even their life trajectories .[71] Finally**,** as mentioned above, eligible students, children and parents are unable to opt out from FRT being used in schools for security purposes because, in accordance with federal guidance, schools could make a unilateral decision to purchase and utilize FRT.

In contrast, the use of FRT for administrative purposes, such as unlocking a device, is not likely to have the same civil rights consequences as those discussed by Barrett and New York University Director of Policy Research Rashida Richardson, because it is unlikely that student FRT data, used for administrative purposes only, would be uploaded or compared to a criminal database.[72] Administrative purposes are more likely to utilize one-to-one processes, which carry less risk of false identification than one-to-many processes, as discussed previously. However, this use could result in other negative consequences, such as loss of access to a device if errors occurred.

The risks for different subgroups could be determined by the type of biometric technology used as well as the amount of data transfer required and could be mitigated depending on how and where the data is stored, including if it is being used on a one-to-one basis. For example, the CISCO platform DUO allows users to create security through the use of biometric data (this platform is used in Apple's Touch ID and FACE ID, as well as Android's fingerprint feature).[73] However, the information is stored only on the device and is never shared with CISCO.[74] This type of biometric information is used on a one-to-one basis, which also could mitigate risk.[75]

(3/16/2023) https://www.nbcnews.com/tech/security/amazon-sued-not-telling-new-york-store-customers-facial recognition-rcna75290, Perez v. Amazon, 23-cv-2251 (S.D. NY, 3/16/2023)

69 The Perpetual Line-Up - Center on Privacy and Technology at Georgetown Law - 121616.pdf; Barrett

70 Barrett

71 Id.

72 Barrett; Rashida Richardson, *Dirty Data, Bad Predictions: How civil rights violations impact police data, predictive policing systems, and justice*, 94 N.Y. U. L. Rev. 15 (2021), https://papers.ssrn.com/sol3/Delivery.cfm SSRN_ID3377428_code3361828.pdf?abstractid=3333423&mirid=1&type=2 (Last Accessed 3/6/2023)

73 *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies*, 86 Fed. Reg. 56300 (10/8/2021) https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for information-rfi-on-public-and-private-sector-uses-of-biometric-technologies (last accessed 3/6/2023) can be found at National Artificial Intelligence Office, *Public Input on Public and Private Sector Uses of Biometric Technologies,* https://www.ai.gov/86-fr-56300-responses/ (last accessed 3/17/2023), the Combined Responses are available in a single document at https://www.ai.gov/rfi/2022/86-FR-56300/Biometric-RFI-2022-combined.pdf (last accessed 3/17/2023)

74 Id.

75 Id.

Administrative vs. Security Uses of Non-FRT BIT

The risks of false identification in non-FRT forms of BIT can be high, depending upon the quality of the technology used as well as the method of collection. As discussed previously, there could be less risk if the BIT is used in one-to-one processes.[76] Furthermore, if the data is collected openly with an individual's consent, there is less chance of error than if the information is collected covertly or from a distance.[77] Because of this, there could be less risk involved if schools were to utilize forms of BIT such as fingerprints, handprints, retina and iris patterns, and DNA sequence, assuming these forms of BIT were collected directly. Additionally, voice and gait identifiers could carry more risk because they could be collected unknowingly from a distance.

Non-FRT forms of BIT are less likely to negatively impact student civil rights and civil liberties when used for security purposes. This would be especially true if schools inform parents and students about the school's intention to use non-FRT forms of BIT for security prior to implementation and obtain parental consent *even if not required to do so*.[78] These precautions will help to ensure that non-FRT forms of BIT are less likely to invade civil rights and liberties.[79] The impact on civil rights and liberties could also be lessened if schools implement policies ensuring that data will not be used in collaboration with law enforcement and instead used only in conjunction with a school database.[80]

Because non-FRT forms of BIT do not utilize facial features, there is less likelihood that student civil rights and liberties will be implicated if these forms of BIT are not shared with or used in collaboration with law enforcement. However, Fourth Amendment privacy may still be implicated, as discussed in 1.a.ii. above. Consensual use of non-FRT BIT could limit infringement on student civil right and liberties.

For example, false identifications in a school lunch setting, such as fingerprints being used for school lunch payments, a known use of BIT in some New York school settings before the passage of STL Section 106-b, do not have the same impact on student civil rights and liberties or level of as BIT used in conjunction with a law enforcement database.[81] This is in part because some forms of BIT, such as fingerprint recognition systems, do not store images of the characteristics being used. Instead, a number is given to a student's fingertip image in the first pass in the biometric device. The number is again generated for subsequent reads and compared with the numbers stored, identifying the student if there is a match.[82] Risk of false identification based on subgroup could be lessened by the use of non-FRT BIT because that technology may not be as reliant on algorithms with possible racial or ethnic bias found in some FRT applications.[83]

---

76 Privacy by Design Solutions for Biometric One-to-Many Identification Systems.pdf

77 Biometric RFI 2022 combined.pdf

78 Marcela Hernandez-de-Menendez, *Biometric Applications in Education*, 48 Int'l J. Interactive Design Mfg. 365 (IJIDeM) (2021) https://link.springer.com/article/10.1007/s12008-021-00760-6, https://link.springer.com content/pdf/10.1007/s12008-021-00760-6.pdf (Last Accessed 3/6/2023)

79 Id.

80 Id.; Beena Ammanath, *Facial Recognition: Here's looking at you*, Deloitte AI Institute (2021) https://www2.deloitte com/content/dam/Deloitte/us/Documents/technology/us-ai-institute-facial-recognition.pdf (Last Accessed 3/6/2023); *Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies*, 86 Fed. Reg. 56300 (10/8/2021) https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies (Last Accessed 3/6/2023)

81 Esther Ledelle Mead, *Privacy and Security Implications of Biometrics in Schools: Should Parents be Concerned?*, 2014 IFIP Dewald Roode Info. Sec. Res. Wkshp. (2014) https://www.researchgate.net/publication/327201058 Privacy_and_Security_Implications_of_Biometrics_in_Schools_Should_Parents_be_Concerned (Last Accessed 3/6/2023)

82 Marcela Hernandez-de-Menendez, *Biometric Applications in Education*, 48 Int'l J. Interactive Design Mfg. 365 (IJIDeM) (2021) https://link.springer.com/article/10.1007/s12008-021-00760-6, https://link.springer.com content/pdf/10.1007/s12008-021-00760-6.pdf (Last Accessed 3/6/2023)

83 Biometric RFI 2022 combined pdf; Stephen Ritter, *Biometrics Aren't Inherently Biased — We're Training Them Wrong*, Forbes (11/4/2020) https://www.forbes.com/sites/forbestechcouncil/2020/11/04/biometrics-arent-inherently biased---were-training-them-wrong/ (Last Accessed 3/6/2023)

Effectiveness for Security

General Considerations

The effectiveness of FRT and non-FRT BIT varies greatly depending upon the application, whether a one-to-one or one-to-many algorithm is used, the population upon whom the technology is used, its intended purpose, and other variables. Many claims have been made about the potential of FRT security systems to make schools safer,[84] but little information is available about real-life situations where technology detected and helped prevent violent incidents. It is noteworthy that, regardless of the type of technology used, a school's staff must have some type of forewarning that an individual should not be allowed access to a school for any technology to be effective. According to researchers at The Violence Project, 70 percent of school shooters from 1980 to 2019 were current students.[85] Neither FRT nor any other BIT would prevent a current student from entering a school building unless an administrator or staff member first noticed that the student was in crisis, had made some sort of threat, or indicated in some other way that they could be a threat to school security.

While FRT vendors claim FRT offers increased school security, FRT may only offer the appearance of safer schools.[86] Indeed, "Averted School Violence (ASV) Database 2021 Analysis Update," issued jointly by the National Police Foundation and the U.S. Department of Justice's Community Oriented Policing Services (COPS) division reiterates that the vast majority of individuals who were thwarted in attempts to perpetrate school violence were current students. Even more telling are the statistics on how those attempts were thwarted: in the vast majority of instances, an intent to perpetrate violence at a school was discovered because the individual: (1) told a peer; (2) posted their intent on social media; or (3) the individual communicated their intent in some other way, allowing an intervention.[87]

Educational researchers point out that reliance on technology to secure schools can lull administrators and staff into a false sense of security when what is really needed is face-to-face interaction with students who may be in crisis.[88] Professor Dewey Cornell, psychologist and educational researcher at the University of Virginia, has been developing his "threat assessment" model for schools since 2001.[89] This method uses staff interaction and assessment with students to

---

84 https://www.tandfonline.com/doi/full/10.1080/17439884.2022.2039938

85 Jillian Peterson, *Presence of Armed School Officials and Fatal and Nonfatal Gunshot Injuries During Mass School Shootings*, United States, 1980-2019, JA<A Netw Open (2/16/2021) https://jamanetwork.com/journals jamanetworkopen/fullarticle/2776515 (last accessed 3/17/2023)

86 Drew Harwell, *Unproven Facial-Recognition Companies Target Schools Promising an End to Shootings*, Washington Post (6/7/2018) https://www.washingtonpost.com/business/economy/unproven-facial-recognition companies-target-schools-promising-an-end-to-shootings/2018/06/07/1e9e6d52-68db-11e8-9e38-24e693b38637 story.html (last accessed 3/17/2023)

87 National Police Foundation, *Averted School Violence (ASV) Database*: 2021 Analysis Update, Washington DC Office of Community Oriented Policing Services (9/2021) https://www.policinginstitute.org/publication/averted-school violence-asv-database-2021-analysis-update/ (last accessed 3/17/2023)

88 Mark Andrejevic and Neil Selwin, *Facial Recognition Technology In Schools: Critical Questions And Concerns*, Learning, Media and Technology v45, Issue 2 pp 115-238 (11/5/2019) https://www.tandfonline.com/doi/full/1 .1080/17439884.2020.1686014 (last accessed 3/17/2023); Nancy Rappaport, *How the School Shooting in Michigan Might have been Prevented*, WBUR Cognoscenti (12/7/2021) https://www.wbur.org cognoscenti/2021/12/07/oxford-high-school-michigan-shooting-nancy-rappaport (last accessed 3/17/2023); Virginia Youth Violence Project, *Threat Assessment Research Publications Compilation 2004-2019*, Virginia Youth Violence Project, https://static1.squarespace.com/static/5ae6702aa2772c3020f1057d/t/60685a3c1c473310b556 cd0/1617451585047/School+threat+assessment+articles+published+2004-2020.pdf (last accessed 3/17/2023)

89 University of Virginia School of Education and Human Development, *The Comprehensive School Threat Assessment Guidelines*, U VA (2018) https://education.virginia.edu/research-initiatives/research-centers-labs/research-labs youth-violence-project/yvp-projects-resources/comprehensive-school-threat-assessment-guidelines (last accessed 3/17/2023); Virginia Youth Violence Project, *Threat Assessment Research Publications Compilation 2004-2019*, Virginia Youth Violence Project, https://static1.squarespace.com/static/5ae6702aa2772c3020f1057d/t/60685a c1c473310b556dcd0/1617451585047/School+threat+assessment+articles+published+2004-2020.pdf (last accessed 3/17/2023)

assess potential threats and stop incidents before they start.[90] This model also puts into practice the methods shown to be effective by the Averted School Violence Database.[91]

A final consideration regarding the use of FRT for security purposes is the fact that students' grown and change during the years typically spent attending school. This makes FRT use on students less effective and could cause consequences (such as barring students from school unnecessarily), which outweigh the potential benefits of FRT security systems.[92]

Administrative vs. Security Use of FRT

Vendors claim that FRT used for security purposes could increase and streamline school safety.[93] While efficiency is helpful, potential inaccuracy could have a detrimental effect on the effectiveness of a school's security and school climate.[94] There is evidence FRT is less accurate for children, elderly, people of color, women, and non-binary people as discussed above, though FRT can be made more accurate through technology and scenario evaluations.[95] Additionally, FRT may not address the underlying causes of school security issues.[85] For example, while FRT could lag potentially dangerous visitors when they enter the school, this may not result in increased police response time if that person decides to do harm.[96] Also, many bad actors in school violence incidents had not been barred from the school prior to the incident.[97]

Biometric applications can be used in a variety of circumstances for both security and administrative purposes. Applications of FRT for security purposes include potentially screening visitors against a known database; tracking visitors, students and staff as they move around a school; disciplining students; and granting access to school buildings or certain parts of school buildings. Schools would likely need prior authorization for the use of these products from SED if the school plans to use the Smart Schools Bond Act Funds for the purchase of the FRT[98]. [99] FRT can also be used for administrative purposes, such as paying for lunches; monitoring student and staff attendance; checking out library books; verifying that students are on the right bus; or unlocking a device, such as an iPad or a computer.[100]

---

90 Id.

91 Id.;

92 Dana Michalski et al, *The Impact of Age and Threshold Variation on Facial Recognition Algorithm Performance using Images of Children,* IEEE 2018 International Conference on Biometrics (2/20-2/23/2018, added to IEEE Xplore on 7/16/2018); Nisha Srinivas et al., *Face Recognition Algorithm Bias: Performance Differences on Images of Children and Adults,* 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (6/16-17/2019, added to EEE Xplore 4/9/2020).

93 US Government Accountability Office, *Facial Recognition Technology: Current and planned uses by Federal Agencies*, GAO-21-526, U.S. Gov't. Accountability Off. (8/2021) https://www.gao.gov/products/gao-21-526 (Last Accessed 3/6/2023)

94 See Barrett

95 Biometric RFI 2022 combined pdf

96 Id.

97 *K-12 School Shooting Database,* https://k12ssdb.org/ (last accessed 3/17/2023); National Police Foundation, *Averted School Violence (ASV) Database*: 2021 Analysis Update, Washington DC Office of Community Oriented Policing Services (9/2021) https://www.policinginstitute.org/publication/averted-school-violence-asv-database 2021-analysis-update/ (last accessed 3/17/2023)

98 See generally: New York State Education Department, Smart Schools Bond Act Implementation Guidance, New York State Education Department (2023) https://www.p12.nysed.gov/mgtserv/smart_schools/docs/Guidance Smart%20Schools_revised_030723.pdf

99 US Government Accountability Office, *Facial Recognition Technology: Current and planned uses by Federal Agencies*, GAO-21-526, U.S. Gov't. Accountability Off. (8/2021) https://www.gao.gov/products/gao-21-526 (Last Accessed 3/6/2023)

100 Rasha Khudiar Rija, Payment Systems Based on Face Recognition: A Survey, 41:5 Guangdianzi Jiguang/J. of

In addition to these uses, however, are less intuitive applications that are already being applied to students: verifying identity for online courses and tests to prevent cheating, as well as facial detection techniques that attempt to measure student engagement.[101] Systems scan for brow-raising, eyelid tightening, and mouth dimpling in order to attempt to gauge whether students are bored, confused, delighted, frustrated, etc.[102]

"Biometric applications can be used in a variety of circumstances for both security and administrative purposes."

Administrative vs. Security Uses of Non-FRT BIT

Non-FRT BIT can be used for security purposes or administrative purposes.[103] Non-FRT BIT can be used to grant building or secure area access, screen visitors, and monitor attendance, as well as for administrative purposes such as making payments (e.g., school lunch payments) or unlocking devices, such as iPads or computers.[104]

Fingerprint scanning has been shown to be effective for making school lunch payments, managing student and staff attendance, and checking out library books.[105] These activities are likely to be performed using a one-to-one algorithm, making them more effective than one-to-many processes.[106] However, frequent student monitoring has been shown to have a negative impact on student mental health.[107] NYS schools have self-reported little or no use of: handprints, retina/iris patterns, DNA sequencing, or voice/gait BIT for biometric identification, making further analysis of the effectiveness of these identifiers necessary only if they become used in schools on a wider scale.[108]

Optoelectronics Laser 563 (5/2022) https://www.researchgate.net/publication/360972928_Payment_Systems Based_on_Face_Recognition_A_Survey (Last Accessed 3/6/2023); Biometric RFI 2022 combined pdf

101 Mark Andrejevic and Neil Selwin, *Facial Recognition Technology In Schools: Critical Questions And Concerns*, Learning, Media and Technology v45, Issue 2 pp 115-238 (11/5/2019) https://www.tandfonline.com/doi/full/10.1080 17439884.2020.1686014 (last accessed 3/17/2023)

102 Id.

103 Jammi Ashok, An Overview of Biometrics, 2 Int'l. J. Comput. Sci. Eng'g. 2402 (2010) https://www.researchgate.net publication/50194220_An_Overview_of_Biometrics (Last Accessed 3/6/2023)

104 US Department of Homeland Security Office of Biometric Identity Management, *Biometrics*, https://www.dhs.gov biometrics (Last Accessed 3/6/2023); Ashok, Overview of biometrics.pdf

105 identiMetrics, *identiMetrics Solutions*, https://www.identimetrics.net/solutions (Last Accessed 3/6/2023); identiMetrics, *How identimetrics Finger Scanning Works*, Newton High School (9/2/2019) https://www.tapinto.net towns/newton/sections/education/articles/newton-high-school-to-use-finger-print-scans-for-security (Last Accessed 3/6/2023)

106 Privacy by Design Solutions for Biometric One-to-Many Identification Systems.pdf

107 Hannah Quay-de la Vallee, *The Chilling Effect of Student Monitoring: Disproportionate Impacts and Mental Health Risks*, Ctr. Democracy Tech. (5/5/2022) https://cdt.org/insights/the-chilling-effect-of-student-monitoring disproportionate-impacts-and-mental-health-risks/ (Last Accessed 3/6/2023)

108 See Exhibit B

Sharing

General Considerations

FERPA generally requires that a school obtain written parental consent if the school wants to disclose PII from a student's educational record to a third-party.[109] This includes BIT data, because FERPA's definition of PII includes a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual,[110] and this definition could apply to both security and administrative use of BIT if the data is made part of the student's educational record. However, as discussed in Section 1.a.i., there are a number of exceptions to the prior written consent requirement that permit schools to disclose PII, but do not *require* schools to do so.[111] One of these exceptions is the "School Official" exception.

Essentially, a school may share PII with an individual or entity designated a "school official" if the school determines that the "school official" has a "legitimate educational interest" in the information.[112] It is noteworthy that, "school official" is not defined in FERPA or its regulations; however the U.S. Department of Education (USDOE) normally interprets this to mean teachers, professors, instructors, administrators, health staff, counselors, attorneys, clerical staff, trustees, members of committees and disciplinary boards, and third-party contractors, volunteers or other parties to whom the school has outsourced institutional services or functions.[113] The requirements to share PII with a third-party determined to be a "school official" are listed in Section 1.a requirements. Thus, although FERPA requires parental consent before releasing confidential information from an education record, schools may share biometric data with "school officials" – such as security system providers – who have a "legitimate educational interest" without first obtaining parental consent. Schools decide who gets to be designated a "school official."[114]

Both FERPA and Section 2-d require schools to provide parents and eligible students an opportunity to inspect and review education records upon request. FERPA requires access within 45 days following receipt of a request. This may include FRT data if it is part of a student's education record.[115]

Additionally, schools may be required to disclose information from a student's education record to courts or litigants in order to comply with a lawfully issued subpoena or judicial order.[116] However, FERPA requires schools to make a reasonable effort to notify the parent or eligible student of the subpoena or judicial order before complying with it, so as to allow the parent or eligible student to seek an order of protection, unless certain exceptions apply.[117]

---

109 United States Department of Education, *An Eligible Student Guide to the Family Educational Rights and Privacy Act (FERPA) SPPO-23-01*, US. Ed. Dept. (3/8/2023), https://studentprivacy.ed.gov/sites/default/files/resource document/file/An%20Eligible%20Student%20Guide%20to%20FERPA_0.pdf (last accessed 3/6/2023); United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https:/ studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (last accessed 3/6/2023)

110 34 CFR § 99.3

111 United States Department of Education, *An Eligible Student Guide to the Family Educational Rights and Privacy Act (FERPA) SPPO-23-01*, US. Ed. Dept. (3/8/2023), https://studentprivacy.ed.gov/sites/default/files/resource document/file/An%20Eligible%20Student%20Guide%20to%20FERPA_0.pdf (last accessed 3/6/2023); United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https:/ studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (last accessed 3/6/2023)

112 Id.

113 Id.

114 Id.; 34 CFR Part 99 ; United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents pdf (last accessed 3/6/2023)

115 34 CFR Section 99.10

116 34 CFR Section 99.31(9)

117 Id.

Section 2-d and Part 121 add additional protections from the release or sharing of PII that exceed FERPA requirements. For instance, Section 2-d does not allow PII to be sold or released for any commercial purpose, and PII provided to third-party contractors cannot be sold or used for marketing purposes.[118] Additionally, PII cannot be shared unless it is for a purpose that would benefit the student and school.[119]

FRT vs. Non-FRT BIT

There is no differentiation between FRT and non-FRT BIT for purposes of sharing PII under any data privacy laws, federal or state. All forms of BIT would fall under FERPA's definition of PII as a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual.[120] The sharing of all BIT data with parents, law enforcement, individuals, litigants, the courts, and any other third parties would be subject to the same implications as any other PII.

118 NYS Educ. L. Section 2-d, 2-d (3) (b) (1) and (f).

119 NYS Educ. L. 2-d (5) (b) (1).

120 United States Department of Education, *An Eligible Student Guide to the Family Educational Rights and Privacy Act (FERPA) SPPO-23-01*, US. Ed. Dept. (3/8/2023), https://studentprivacy.ed.gov/sites/default/files/resource document/file/An%20Eligible%20Student%20Guide%20to%20FERPA_0.pdf (last accessed 3/6/2023); 34 CFR 99.3; United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (last accessed 3/6/2023)

Administrative vs. Security

The analysis regarding whether it is permissible to share PII (whether FRT in particular or BIT as a whole) with third-parties does not turn on the purpose for which it is being used by the school, but instead on why it is being shared with that third-party.[121] Therefore, considerations regarding whether PII can be shared with third-parties are universal and will not be different depending upon application as long as the data is being shared for a "legitimate educational purpose."

Sharing FRT or Non FRT BIT with Law Enforcement

During stakeholder meetings, particular concern was expressed regarding the sharing of FRT with law enforcement. If the Commissioner authorizes FRT use, schools must continue to abide by the privacy requirements imposed by FERPA, including those regarding law enforcement. Additionally, as part of the feedback provided to ITS by stakeholders, DCJS noted that it is important to ensure biometric data is only being used and/or accessed for its intended purpose. This opinion is based on the agency's experience with sharing biometric information (such as fingerprints) in the criminal justice space, which is highly regulated through Federal policy, such as CJIS (Criminal Justice Information Services). Also in this process, DOCCS raised the importance of conducting regular assessments and assessing recommendations for product upgrades and improvements as to accuracy of FRT.

Many schools utilize school resource officers (SROs) to assist with ensuring safety and preventing crime in schools. SROs serve as on-site law enforcement officers and liaisons with the local police or sheriff's office. SROs may be employed by the school, local police department, or sheriff's office.[122] Education Law Section 2801-a (10) requires schools to enter into a written contract or a memorandum of understanding (MOU), developed with stakeholder input, between the school district and the law enforcement entity or public or private security personnel, including SROs.

Although an SRO may be designated by a school as a "law enforcement unit" official under FERPA, in order for a school to disclose PII to an SRO without parental consent the disclosure must fall within the "school official" with a "legitimate educational interest" exception as discussed in Section 1(a)(i).[123] The legitimate educational interest would be to promote school security and the physical safety of students[124]. When receiving PII under the school official exception, SROs, like other school officials, are prohibited from redisclosing PII to others.[125]

SROs and other members of a school law enforcement unit may create their own records for law enforcement purposes; these records are considered "law enforcement unit records."[126],[127] Even though they are created and maintained in a school environment, "law enforcement unit records" are created and maintained by law enforcement, not educators, and are therefore not "education records" subject to the protections of FERPA. As a result, these records *may* be disclosed to

---

121 See generally FERPA and NYS Educ. L. Section 2-d

122 US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https:/studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

123 United States Department of Education, *FERPA General Guidance for Students*, US. Ed. Dept. (4/2020) https:/studentprivacy.ed.gov/sites/default/files/resource_document/file/FERPAforeligiblestudents.pdf (last accessed 3/6/2023)

124 Id.

125 20 USCA 1232g(b)(1)(C) and 34 CFR 99.8; NYS Educ. Law Section 2-d(5)(f)(3)(ii) and 8 NYCRR 121.9 and see US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

126 US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

127 US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https:/studentprivacy.ed.gov sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

third parties without parental consent.[128] Schools may, however, disclose PII from education records when it is determined that there is a health or safety emergency, and the disclosure is necessary to protect the health or safety of students or other individuals.[129] The USDOE has provided guidance that these disclosures must be related to a significant and articulable emergency such as an impending natural disaster, a terrorist attack, a campus threat, or the outbreak of an epidemic disease.[130]

Sharing non-FRT BIT data with law enforcement would be subject to the same implications as FRT data under FERPA.

Storage of FRT and Non FRT BIT Data

The NYS Archives has authority over retention and disposition of school districts' and BOCES's records (including charter schools but not non-public schools).[131] This authority would include biometric data and related information if the use of these technologies is authorized by the Commissioner. The Retention and Disposition Schedule for New York Local Government Records (LGS-1) is the comprehensive records retention schedule developed by the Archives.[132] Educational agencies are required to pass a resolution adopting the LGS-1.[133],[134] Although the LGS-1 does not specifically address the retention of biometric data, Sections 811 and 846 provide three-year retention periods for facility security records, including video or audio records maintained for security purposes.[135]

Schools that decide to use BIT, for whatever purpose, will do so by purchasing biometric technology products and services. Third-party vendors and contractors who are provided access to PII via these purchases must, in accordance with Section 2-d, enter into written contracts with schools. In circumstances wherein schools determine that contractors are "school officials" with "legitimate educational interests" under FERPA, schools are required to maintain direct control over the use and maintenance of education records.[136] Therefore, schools have been and would continue to be expected to address data retention and destruction of all BIT and other data related to all third-party contracts to ensure the privacy and security of PII from education records.

When biometric data and information no longer needs to be retained, either in accordance with the LGS-1 for schools or per the terms of a contract with third-party contractors and vendors, destruction should be undertaken as soon as possible to ensure proper asset management. Under Section 2-d and Part 121.5(b), schools are required to implement a data privacy and security policy that aligns with the NIST Cybersecurity Framework (CSF), which advises proper data destruction

---

128 US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

129 20 USC 1232g(6)(b)(1)(I); see US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023)

130 see US Department of Education Privacy Technical Assistance Center (PTAC), *School Resource Officers, School Law Enforcement Units, and the Family Educational Rights and Privacy Act (FERPA),* US Educ. Dept. (2/2019) https://studentprivacy.ed.gov/sites/default/files/resource_document/file/SRO_FAQs.pdf (last accessed 3/17/2023))

131 NY Art. & Cult. Aff. Section 57.05

132 See generally: NYS Archives Records Management available at: NYS Archives, *Local Government Schedule: LGS-1*, NYS Archives (4/1/2022) http://www.archives.nysed.gov/records/local-government-record-schedule/lgs-1 title-page (Last Accessed 3/6/2023)

133 8 NY ADC App. L

134 NYS Archives, *Local Government Schedule: LGS-1*, NYS Archives (4/1/2022) http://www.archives.nysed.gov records/local-government-record-schedule/lgs-1-title-page (Last Accessed 3/6/2023)

135 Id.

136 20 USC 1232g

when the data is no longer in use.[137] Therefore, as part of their asset management program, schools should have policies in place that address the proper disposal and sanitization of confidential data, especially PII from education records. As the retention and disposal of PII or BIT may be different from other records retention and disposal requirements, such as those related to student enrollment or graduation, schools should ensure segregation of any BIT-related records from other educational records.

Risk of Breach of FRT and non FRT BIT Data

Section 2-d and Part 121 require schools to implement and maintain data privacy and security policies that align with the NIST CSF in order to protect data. PII from educational records, including BIT, is confidential information that must be kept secure via these protocols. However, despite best efforts, data breaches do occur. If the Commissioner authorizes schools to use FRT or non-FRT BIT, breaches may include biometric data. The unauthorized disclosure of BIT, especially FRT, is particularly problematic because BIT cannot be changed to protect the individual in the same way a credit card number might be changed after a breach. Once an individual's fingerprint or FRT data is disclosed, the damage is permanent.

School vendors, rather than schools themselves, were the primary victims of all K-12 school data breaches reported to the Kindergarten Through Twelfth Grade Security Information Exchange (K-12 SIX) between 2016 and 2021.[138] Section 2-d and Part 121 require that third-party contractors report breaches of PII to the school they provide services for under contract. In turn, the school is required to report the breach to SED's Data Privacy Office. A school must notify affected parents and eligible students of an unauthorized disclosure no more than sixty calendar days after the discovery of the breach.[139] If the breach is attributed to the third-party contractor, the contractor must reimburse the school for the cost of notification.[140]

Although most education record breaches do not currently fall under the purview of STL section 208 or General Business Law Section 899-aa (also known as the Shield Act), these laws specifically list "biometric information" as a data element of private information. Therefore, if the Commissioner authorizes schools to use BIT, a breach of that data may also require a school's third-party contractor to comply with these laws.[141] Additional requirements under these laws include notification

---

137 NIST, *Getting Started with the NIST Cybersecurity Framework*, NIST Sp. Pub. 1271 (8/2021) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1271.pdf (last accessed 3/17/2023)

138 Cybersecurity and Infrastructure Security Agency, *Protecting Our Future: Partnering to safeguard k–12 organizations from cybersecurity threats*, US DHSES CISA (1/2023) https://www.cisa.gov/sites/default/files/2023-01/K-12reportFINAL_V2_508c.pdf (last accessed 3/17/2023); Levin, Douglas A, *The State of K-12 Cybersecurity: Year in Review – 2022 Annual Report*, K12 Security Information eXchange (2022) https://www.k12six.org/the-report (last accessed 3/17/2023)

139 8 NYCRR 121.10 (e)

140 8 NYCRR 121.10 (f)

141 NYS GBL Section 899-(2) (b) (4)

to the affected individuals, notification to the NYS Attorney General's office, and potentially, paying for credit monitoring for those affected by the breach.[142] [143] Furthermore, pursuant to Section 2-d and Part 121, consequences could be imposed on a third-party contractor if it is determined that the contractor knowingly or recklessly allowed for the unauthorized disclosure of student data. Penalties may include barring the third-party contractor from accessing student data for a fixed period of up to five years, requiring additional training at the contractor's expense, and imposing a civil penalty that aligns with General Business Law Section 899-aa.[144]

Section 2-d (7) (c) states there is no private right of action against SED or a school under Section 2-d. However, a cause of action under other legal theories, such as negligence, could be possible.

For individuals affected by a BIT data breach, the main disadvantage is that biometric data cannot be changed, and data breaches will always remain connected to specific individuals. If a breach is not discovered for an extended period of time, hackers could commit numerous malicious activities before getting caught.[145] For example, in 2019, researchers infiltrated Suprema's BioStar 2 system and accessed over 27.8 million records, including fingerprints and photos of faces.[146]

Many forms of BIT, such as fingerprints, are immutable,[147] and disclosure of this data could put users at permanent risk. The risk remains high that a breach of BIT might result in the disclosure of physical characteristics that cannot be replaced.[148]

Cost of FRT and Non-FRT BIT

An FRT system includes five main parts: hardware, connectivity technology, FRT software, a database of faces, and a user interface.[149] A limited functionality system can cost a few thousand dollars, but a highly complex, secure system will likely cost $1 million or more.[150] For example, Lockport Central School District (Lockport) spent $1.4 million on an FRT security system by AEGIS for a district of 4,400 students with an annual budget of $100 million.[151] Specific costs of maintenance and storage would vary depending on such considerations as the population of the purchasing school and the type of technology being purchased. The maintenance and storage costs of other forms of BIT may be less than FRT.[152]

---

142 NYS Ed Law 2-d(6), 8 NYCRR 121.4, 8 NYCRR 121.10, NYS Technology Law 208, NYS General Business Law Section 899-aa(8)(a).

143 There may be slight variations in the definition of "biometric information" as applied to Section 2-d, NYS Technology Law 208, and NYS GBL Section 899-aa(8)(a). Further analysis may be needed to determine whether the definition is met depending upon which law applies.

144 NYS Educ. L. 2-d(6), 8 NYCRR 121.4, 8 NYCRR 121.10

145 Identity Management Institute, *Biometric Data Breach Security Threats*, (2/25/2020), Identity Mgmnt. Inst., https://identitymanagementinstitute.org/biometric-data-breach-security-threats/ (Last Accessed 3/6/2023)

146 Id.

147 Lenildo Morais,*Biometric Data: Increased Security and Risks,* Sec. Mag. (May 6, 2020) https://www securitymagazine.com/articles/92319-biometric-data-increased-security-and-risks (Last Accessed 3/6/2023).

148 Id.

149 Nadejda Alkhaldi, *How much does it cost to create a facial recognition system?*, ITRex Group (2/24/2022) https://itrexgroup.com/blog/how-much-does-a-facial-recognition-system-cost/Last Accessed 3/6/2023)

150 Id.

151 Jim Shultz, Opinion Spying on Children Won't Keep Them Safe, The New York Times (6/7/2019) https://www.nytimes.com/2019/06/07/opinion/lockport-facial-recognition-schools.html?smtyp=cur&smid=tw-nytopinion (Last Accessed 3/6/2023)

152 Danny Thakkar, *Biometric Devices: Cost, types and comparative analysis*, Bayometric https://www.bayometric.com/biometric-devices-cost/ (last accessed 3/17/2023)

School districts are subject to competitive bidding requirements under General Municipal Law Section 103 (1) and Education Law Section 1619, 2513 and 2556 (10), meaning that they must advertise for sealed bids and award contracts to the lowest responsible bidder for public works contracts that exceed $35,000 and purchase contracts that exceed $20,000. Not only must a school purchase the hardware and software to use BIT systems, but it must also pay to maintain the equipment, keep up on subscriptions, and maintain cybersecurity standards. A breach of BIT data will be costly to a school and third-party contractor.

Schools self-report challenges in providing enough funding and staffing to provide robust cybersecurity, and they are increasingly a target of bad actors because schools have a lot of rich data.[153] Many schools lack a chief information security officer (CISO) and the sophisticated expertise required to adequately protect data.[154] According to the Multi-State Information Sharing & Analysis Center's (MS-ISAC) "K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year," 29 percent of the ISAC's members reported being victims of a cyber incident.[155] Data incidents can cause significant monetary loss to both schools and individual victims, as well as loss of learning while systems are down. Notification to parents and eligible students affected by the breach, potential credit monitoring and recovery costs associated with restoring computers, recovering data, and shoring up systems to prevent future attacks can add up to an excessive amount of unexpected costs. In addition to any financial impact, schools could suffer reputational consequences were they to suffer a data breach.[156] Finally, insurance costs for cybersecurity insurance could increase as well or become unattainable – in 2021, ransomware attacks cost schools $3.65 billion in the United States.[157]

Analysis of Other Schools

General Considerations

SED conducted a survey of the educational agency use of biometrics in which schools were asked about various types of BIT they used.[158] The educational agencies surveyed, as defined under Section 2-d, included public elementary and secondary schools, state approved private schools for special education, charter schools, and preschools. SED sent the survey to the data protection officer of each educational agency in NYS and asked various questions about whether and how BIT was being used. The results of the study point out that schools may use FRT and other forms of BIT in various ways. As a result, schools that use FRT or other forms of BIT for administrative purposes to unlock a device or make a payment may have a different costs and efficacy analysis associated with that type of use than if it were used for security purposes. SED would need to publish further materials about the cost of varying uses of the technology in order for the cost and efficacy to be analyzed further.

For example, Lockport CSD's system utilized closed circuit cameras to take biometric measurements of all faces that appear in the frame of the cameras.[159] The system then analyzed facial images through a one-to-many process and compared

---

153 Multi-State Information Sharing and Analysis Center, *K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year*, MS-ISAC (11/2022) https://learn.cisecurity.org/k-12-report (last accessed 3/17/2023); Cybersecurity and Infrastructure Security Agency, *Protecting Our Future: Partnering to safeguard k–12 organizations from cybersecurity threats*, US DHSES CISA (1/2023) https://www.cisa.gov/sites/default/files/2023-01/K-12report FINAL_V2_508c.pdf (last accessed 3/17/2023)

154 https://www.cisa.gov/sites/default/files/publications/K-12report-24Jan23.pdf

155 Multi-State Information Sharing and Analysis Center, *K-12 Report: A Cybersecurity Assessment of the 2021-2022 School Year*, MS-ISAC (11/2022) https://learn.cisecurity.org/k-12-report (last accessed 3/17/2023)

156 Rebecca Torchia, *What Do K–12 IT Leaders Need to Know About Cyber Liability Insurance for School Districts?*, EdTech Mag. (8/4/2022) https://edtechmagazine.com/k12/article/2022/08/what-do-k-12-it-leaders-need-know about-cyber-liability-insurance-school-districts-perfcon (Last Accessed 3/6/2023)

157 Paul Bischoff, *The Best Apps to Encrypt Your Files Before Uploading to the Cloud*, Comparitech (10/11/2018) https://www.comparitech.com/blog/information-security/school-ransomware-attacks/ (Last Accessed 3/6/2023)

158 Exhibit B

159 Shultz v NY State Educ. Dept., 2021 NY Slip Op 33434[U] [Sup Ct, Albany County 2021])

them with a database of non-students who have been determined by Lockport CSD to be a threat to the school.[160] The system then reported any matches to appropriate district officials for verification.[161] This type of system could warrant a different analysis than schools that use FRT or other forms of BIT for administrative purposes.

FRT vs. non-FRT BIT

All NYS school districts are required to have a data protection officer (DPO) who is responsible for the implementation of policies and procedures required by Education Law Section 2-d.[162] SED maintains a listserv of all DPOs. In preparation for this report, SED conducted a survey of all DPOs on its listserv regarding the use of BIT systems. Of 212 respondents, seven reported that they have used FRT, and five of those seven reported that they used FRT for the purpose of teacher and staff attendance only. Some respondents stated that they had used FRT as device security (i.e., facial identification for tablets). When asked whether their school district would consider the use of FRT in the future, 54% of the respondents stated that they might, 22% stated that they would and 24% stated that they would not. Security reasons were the main reason for interest in the use of FRT.[163]

Laws regulating the use of FRT in schools are rare.[164] Some U.S. states and cities have banned or restricted FRT within their geographical confines, but these policies are not school-specific.[165] The French and Swedish governments have determined that FRT is not authorized in schools under the General Data Protection Regulation (GDPR), a law which protects data privacy in the European Union (EU), but FRT is allowed in schools elsewhere in the EU under the same law.[166] Nations in Europe and Africa have nationwide policies regarding the use of FRT, but they are not school-specific.[167]

Several schools in NYS were using fingerprint scanning technology from the company identiMetrics, Inc. prior to NYS's BIT moratorium.[168] [169] identiMetrics provides a unified biometric ID management platform which allows single sign-on ID for administrative applications.[170] These administrative applications include student attendance, tardy management, staff time and attendance, food service, and library service.[171]
identiMetrics does not use actual fingerprints. Instead, it uses digitized templates that are numeric representations of

160 Id.

161 Id.

162 NYCRR Section 121.8

163 Exhibit B

164 Claire Galligan et al, *Cameras in the Classroom: Facial recognition technology in schools*, University of Michigan (8/25/2020) https://stpp.fordschool.umich.edu/research/research-report/cameras-classroom-facial-recognition-technology-schools (last accessed 3/17/2023); NYS's STL 106-b had been passed by the legislature, but not yet signed into law by the Governor at the time the report was published.

165 Id.

166 Id.

167 Id.

168 identiMetrics, *identiMetrics Solutions*, https://www.identimetrics.net/solutions (Last Accessed 3/6/2023);

169 *New York State Accounts Prior to Moratorium*, identiMetrics, Exhibit B

170 identiMetrics, *identiMetrics Solutions*, https://www.identimetrics.net/solutions (Last Accessed 3/6/2023);

171 Id.

individual fingerprints.[172] When a student's fingerprint is scanned into the identiMetrics system, computer software creates a grid of intersection points from the swirls and arcs of the scanned finger.[173] A unique template is then created showing the intersection of unique points on the finger, and the original fingerprint image is destroyed.[174] The template is then converted into a binary number, and the binary number is encrypted and stored.[175]

When a student scans their finger to perform an administrative function through identiMetrics, such as paying for a school lunch, the finger scanning software compares the new template with other templates in the database.[176] When a matching template is found, the student is identified, and payment is made.[177] According to identiMetrics, the identification and matching process takes under one second to complete, and it significantly increases the operational efficiency of such administrative applications.[178,179] identiMetrics' privacy protections state their digitized template cannot be reverse engineered to reconstruct actual fingerprints.[180]

As stated above, in preparation for this report, NYSED conducted a survey of all DPOs on its listserv. Of 212 respondents, 42 reported that they had used non-FRT BIT systems, and seven reported that they have not used BIT. Most schools responded that they use non-FRT BIT for device access, time and attendance, and lunch payment. Some respondents pointed out that use of fingerprint recognition is of great assistance to provide access to computers for students who are too young or otherwise unable to reliably memorize a password.

Impact of Using Existing Databases

General Considerations

STL 106-b requires this report to consider "appropriateness and potential implications of using any existing databases, including but not limited to, local law enforcement databases" in conjunction with BIT systems. Because it is not clear whether "existing databases" is meant to include school databases or vendor databases, we will consider both, together with law enforcement databases. There are pros and cons to each approach, but any database is at risk for breach, whether due to attack by bad actors or due to system or human error. The impact of using other databases for FRT could differ depending on the type of database used. Which databases schools use would be a policy determination to be made in accordance with General Municipal Law, FERPA, Section 2-d and the schools data privacy and security policies.

---

172 identiMetrics, *How identimetrics Finger Scanning Works*, Newton High School (9/2/2019) https://www.tapinto.net/towns/newton/sections/education/articles/newton-high-school-to-use-finger-print-scans-for-security (Last Accessed 3/6/2023)

173 Id.

174 Id.

175 Id.

176 Id.

177 Id.

178 Id.

179 identiMetrics, *identiMetrics Solutions*, https://www.identimetrics.net/solutions (Last Accessed 3/6/2023);

180 *Identimetrics Privacy Protections FAQs*, identiMetrics, Exhibit B

School Databases

Schools may lack funding or staff to create the required cybersecurity protocols. Tasking schools with maintaining databases filled with sensitive BIT could further exacerbate lack of funding or other resources, requiring hiring additional staff or consultants.

Vendor Databases

As mentioned above, vendors were the primary victims of all K-12 school data breaches reported to the Kindergarten Through Twelfth Grade Security Information Exchange (K-12 SIX) between 2016 and 2021. While vendors may be in a better position financially and personnel-wise, with expert staff devoted to data security, they are still at risk for breach. Schools must rely on vendors' assurances that they will comply with student data privacy laws, data protection agreements, and contractual promises that they will protect student PII. In addition, when a breach occurs, the school must rely on the vendor for information in order to report and respond to the incident. Depending on where the vendor stores information, the vendor may have various local laws that may contain stronger or weaker required protections, which may require schools to carefully consider where any vendor records are stored.

Law Enforcement Databases

Schools could utilize law enforcement databases to store FRT in a similar way to how law enforcement databases are accessed through vendors for employment background checks.[181] Schools could check students, staff, or visitors against a law enforcement FRT database coordinated by a vendor. This would put the onus on the vendor and the law enforcement entity to maintain and protect the BIT. However, studies have shown that using law enforcement databases in this way could result in staff or members of the public being falsely matched to someone who is in a criminal database. The likelihood of this error is increased for people of color, women, children, the elderly, and nonbinary people. Furthermore, the use of a law enforcement database could impact the privacy rights of the students, staff and visitors at a school using BIT. Of note, although specifically asked, none of the respondents to the survey conducted by SED reported that their FRT system was connected to law enforcement.[182] Finally, sharing students' FRT with law enforcement could impact their students' privacy rights as set forth under FERPA, and Section 2-d.

The utilization of law enforcement databases for non-FRT BIT could have similar impacts as FRT. However, per SED there is little to no evidence of law enforcement databases having been used for other forms of BIT for either security or administrative purposes in NYS schools, other than Lockport.[183]

Auditing[184]

For Data Security

Under current Education Law, which favors local control, individual schools would decide whether audits should be performed on BIT systems.[185] As described in Section 7 above, schools are subject to the competitive bidding requirements of the General Municipal Law and must also enter into Section 2-d contracts, which include data protection agreements before sharing PII with a third-party contractor. In order to facilitate compliance with the requirements of Section 2-d, SED

181 Consumer Financial Protection Bureau, Market Snapshot: Background Screening Reports, US CFPB (10/2019) https://files.consumerfinance.gov/f/documents/201909_cfpb_market-snapshot-background-screening_report.pdf (Last Accessed 3/6/2023)

182 Exhibit B

183 Exhibit B

184 ITS is interpreting this language to mean possible ways in which auditing could be conducted. The examples in this section are not intended to be a recommendation, but rather the possible ways in which this technology could be hypothetically audited.

185 As well, the State Comptroller has broad audit authority pursuant to Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

has provided guidance to schools in the form of a model Data Protection Agreement that includes a section requiring the contractor to perform a cybersecurity audit at the school's request.[186] Per SED, SED does not currently have the authority to mandate such audits but does recommend them.

For Accuracy

Schools could request audits of FRT systems' false positive rates, especially with respect to race, gender, and age. Schools could also request information on vendors' internal testing of technology, including any scenario evaluations that might have been conducted to increase the accuracy of FRT.[187] Technology evaluations involve isolating particular biometric system components, such as a matching algorithm, and conducting exploratory testing on static datasets, often for the purpose of improving an engineering process.[188] Scenario evaluations measure the performance of end-to-end systems, in real time, on human participants. Scenario evaluations are designed to be externally valid, meaning the simulated performance measured is designed to estimate real world performance. This makes performance data from scenario evaluations more applicable to the task of selecting which biometric systems should be considered for operational deployment.[189] Both types of biometric testing are useful to show the potential limitations of the system. Scenario evaluations are the best for reducing the system's error rate. It is not clear whether a school has the knowledge or the resources to audit the FRT for false positives, or if a self-audit or third-party audit would be required at the request of the school as part of the terms and conditions of the contract.

Biometric testing and accuracy assessments could be conducted on non-FRT forms of BIT as well. Technology and scenario evaluations could be used to audit and improve other forms of BIT utilized by schools in the same ways as FRT.

Disclosure

New York does not currently have comprehensive legislation addressing the use of biometric technologies on its residents, their right to be made aware of the use of biometric technology, or their right to opt-out of such use. Parents and eligible students may not be aware that schools are utilizing FRT or non-FRT BIT, since schools are not required to obtain consent before providing PII to third party contractors providing education services. However, Section 2-d requires schools to publish on their websites the data privacy agreements of the third-party contractors with which it shares PII.[190] The data privacy agreement (DPA) must indicate the exclusive purpose for which the school is disclosing the PII to the vendor. Section 2-d is not applicable to adult biometric information, but adults have other, limited privacy rights, such as those provided by NYS Personal Privacy Protection Law that could limit how a school discloses FRT or other BIT information for adults.[191]

Publishing DPAs on a school's web site, however, may not provide enough transparency for a community. In litigation brought against Lockport and SED, parents alleged that Lockport did not thoroughly engage parents, students, and teachers in the process of installing facial recognition in its school.

---

186 NYS Education Department, *Data Privacy and Security Model Forms and Policies*, NYS Educ. Dept. (2020) http://www.nysed.gov/data-privacy-security/model-forms-and-policies(last accessed 3/17/2023), section 5

187 Yevgeniy Sirotin, *Demographic Variation in the Performance of Biometric Systems: Insights gained from large scale scenario testing*, U.S. Dept. Homeland Sec. (3/31/2021) https://www.dhs.gov/sites/default/files/publications/21_0708_st_demographic_variation_performance_biometric_systems.pdf (Last Accessed 3/6/2023)

188 Jacob A. Hasselgren, *A Scenario Evaluation of High-Throughput Face Biometric Systems: Select Results from the 2019 Department of Homeland Security Biometric Technology Rally*, U.S. Dept. Homeland Sec., Sci. Tech. Dir., Biometric and Identity Tech. Ctr. (8/2020) https://www.dhs.gov/sites/default/files/publications/2021_st-01_2019selectrallyresultstip20201104revised_3046.pdf (Last Accessed 3/6/2023)

189 Id.

190 NYS Educ. L. §2-d(3)(c), 8 NYCRR 121.6

191 Id.

Legislative Impact

FRT and non-FRT BIT data is PII as defined by FERPA and Section 2-d; 34 CFR section 99.3 states that PII includes biometric records that measure biological or behavioral characteristics that can be used for automated recognition of an individual.[192] Therefore, the maintenance of records related to the use of all BIT, the protection of the privacy interests of those whose BIT data is being used, and any breaches of this data will be implicated and be governed by Section 2-d, because FERPA does not contain specific requirements for data breaches. Breaches of any BIT data could impact STL Section 208, as well as the breach notification requirements in General Business Law Section 899-aa as discussed in Section 6 of this report.

Guidance and Recommendations

This report demonstrates that any use of BIT needs to be evaluated against the costs, benefits, and risks of the proposed usage. Notably, for certain BIT that has not been utilized in school settings, additional evaluation may need to be done. This report offers the following conclusions and guidance.

FRT:

Based upon the information collected and the analysis conducted above, there are concerns regarding the use of FRT in public, nonpublic, elementary, secondary, and charter schools in New York State. While there can be benefits to the use of FRT in a school setting, the research conducted and reviewed for this report shows there are discernable risks to the use of this technology in school settings. These risks may outweigh any documented benefits discussed above, and given that the research shows that there may be limitations on the ability to reduce these risks, caution should be used in implementing this technology. As this technology is continuously evolving, schools should revisit any policies or limitations on a frequent basis to determine if changes are needed.

While schools should use caution in use of FRT, especially for security reasons, FRT is also becoming increasingly common for one-to-one device security and management, such as unlocking a device (i.e. a tablet). Based on the research and outreach discussed above, the risks associated with this type of FRT are lower, and there appear to be benefits for use of this technology for younger children or students that may struggle to use a password or other security features. Schools may want to consider allowing this type of FRT, even if more stringent uses of other types of FRT are implemented.

Non-FRT BIT:

The use of digital fingerprinting in public, nonpublic, elementary, secondary, and charter schools in New York State should be left up to local educational agencies that are currently using, or wish to use, this form of Non-FRT BIT in the future. The research conducted and reviewed shows the use of digital fingerprints can be beneficial in school settings. Notably, the risks associated with the use of digital fingerprints are minimal compared to FRT, but still do exist. However, any specific risks may depend on the way this technology is applied.

Based on the research collected, the use of handprints, retina and iris patterns, DNA sequencing, voice, and gait in school settings is rarely implemented in public, nonpublic, elementary, secondary, and charter schools in New York State, if at all.[193] This report is unable to draw conclusions regarding usage of these technologies at this time given the lack of usage. If these forms of Non-FRT BIT become more widespread in the future, further research and analysis will be warranted.

As noted above, non-FRT BIT is increasingly being used for one-to-one device management. Similar to FRT uses, this technology may have particular benefit to students unable to use a password or other security features, and the risks associated with the use are reduced. Therefore, schools may consider allowing this use of non-FRT BIT, even if the schools choose to limit other uses.
As previously noted, ITS acknowledges the ever-changing nature of the technology being examined, and the conclusions reached by this report may need to be reevaluated on an ongoing basis.

---

192 34 CFR 99.3, NYS Ed Law 2-d(1)(d).

193 Exhibit B

Exhibits

The following are survey results from the general survey ITS conducted, and survey results from SED's educational use survey.

ITS Use of Biometric Identifying Technology in Education Study Results

Exhibit A

- 995 complete survey responses.
- 1072 partial responses.

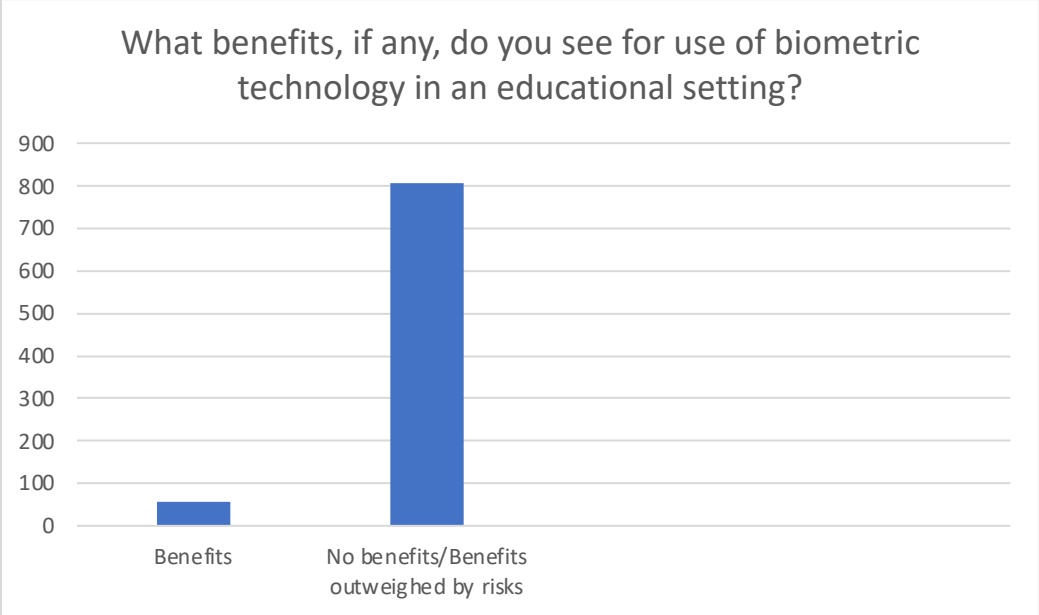
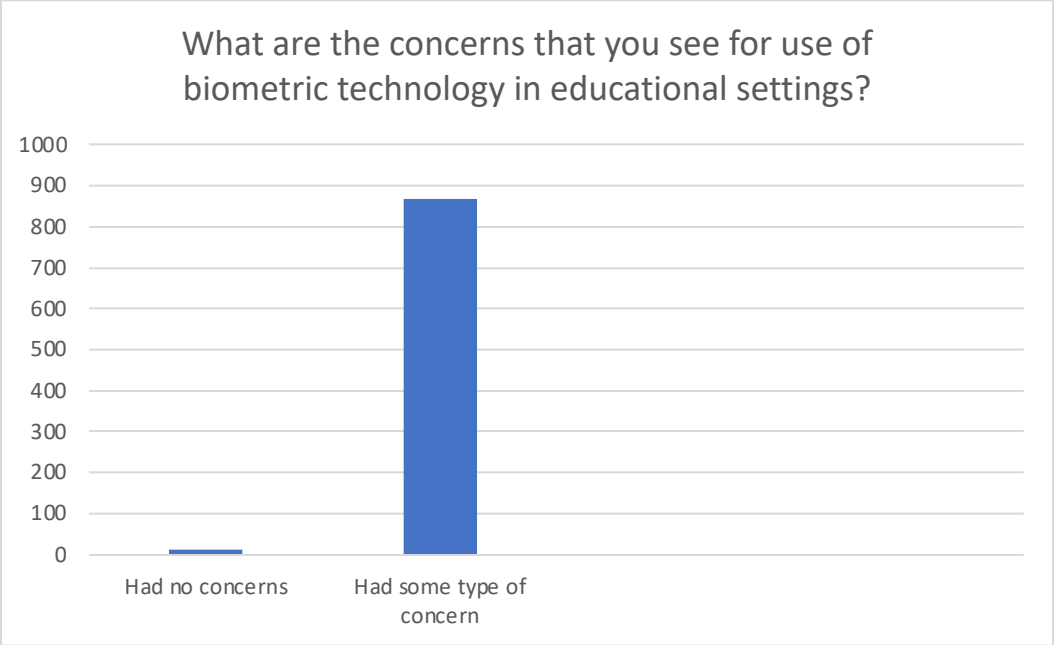


Exhibit B

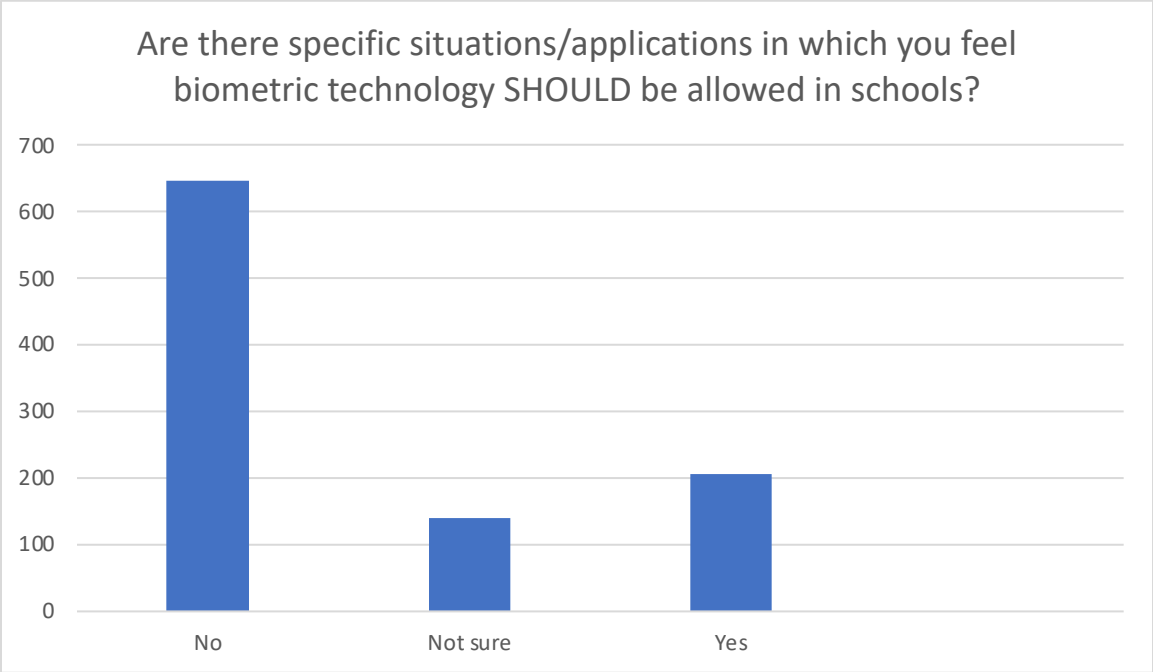
What benefits, if any, do you see for use of biometric technology in an educational setting? (Most frequent responses)

- Helps with recognition of students/staff.
- Keeps unauthorized individuals out of the school.
- Increases safety.
- Minimizes fraud.
- Benefits are outweighed by risks



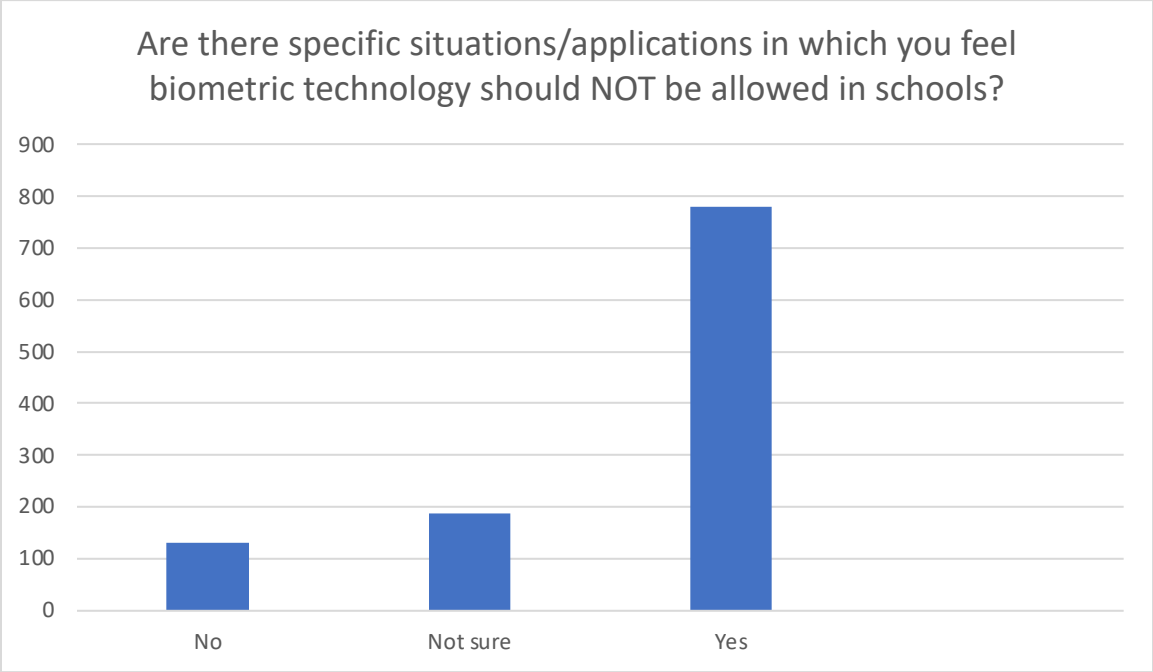
What are the concerns that you see for use of biometric technology in educational settings? Most frequent responses)

- Privacy
- Data breach
- Constitutionality
- Discrimination
- Poor use of funding



In which specific situations/applications SHOULD biometric technology be used? Most frequent responses)

- To screen visitors
- Logging into devices
- Fingerprint scanning for lunch.
- Building access.
- Attendance

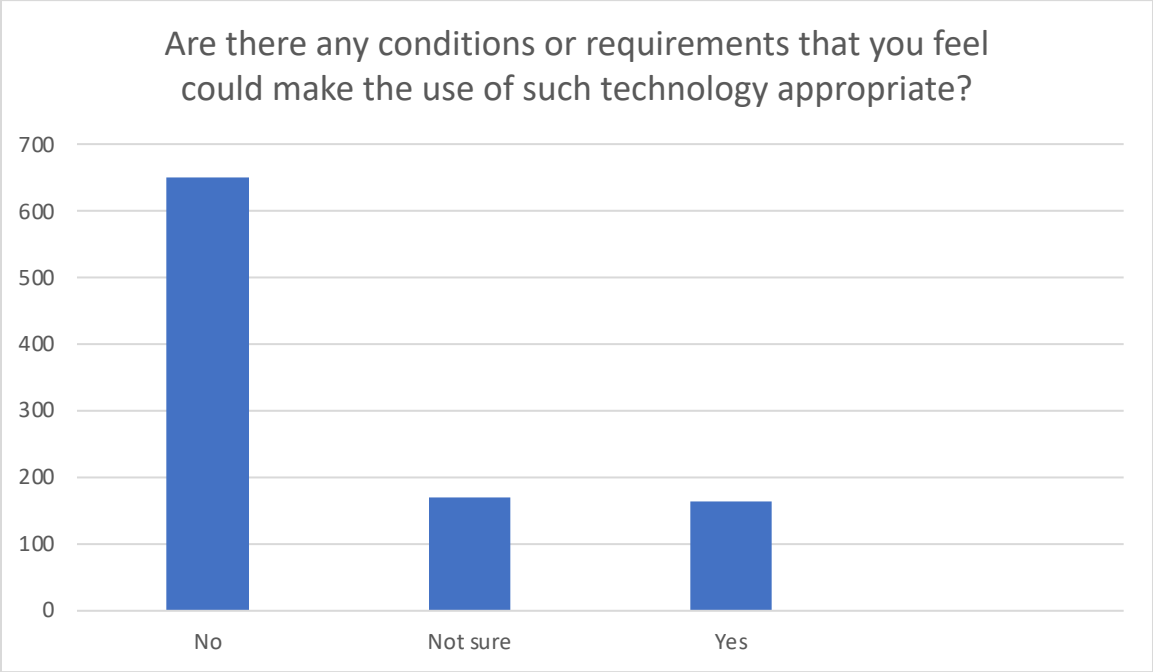


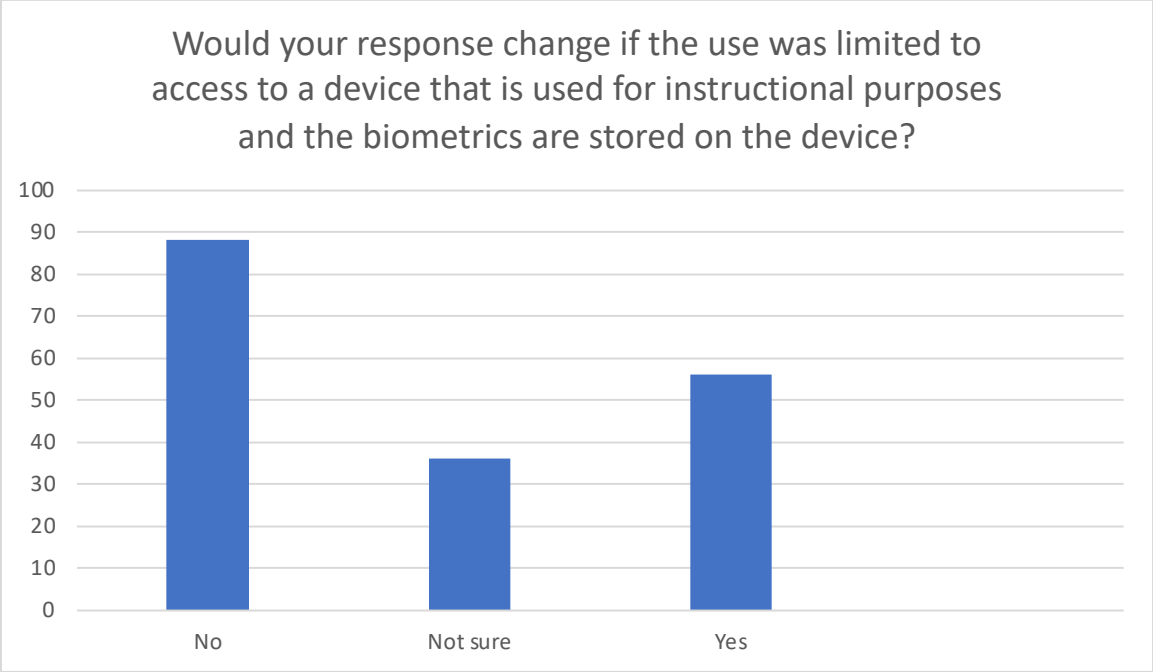
In which specific situations/applications should biometric technology NOT be used? (Most frequent responses)

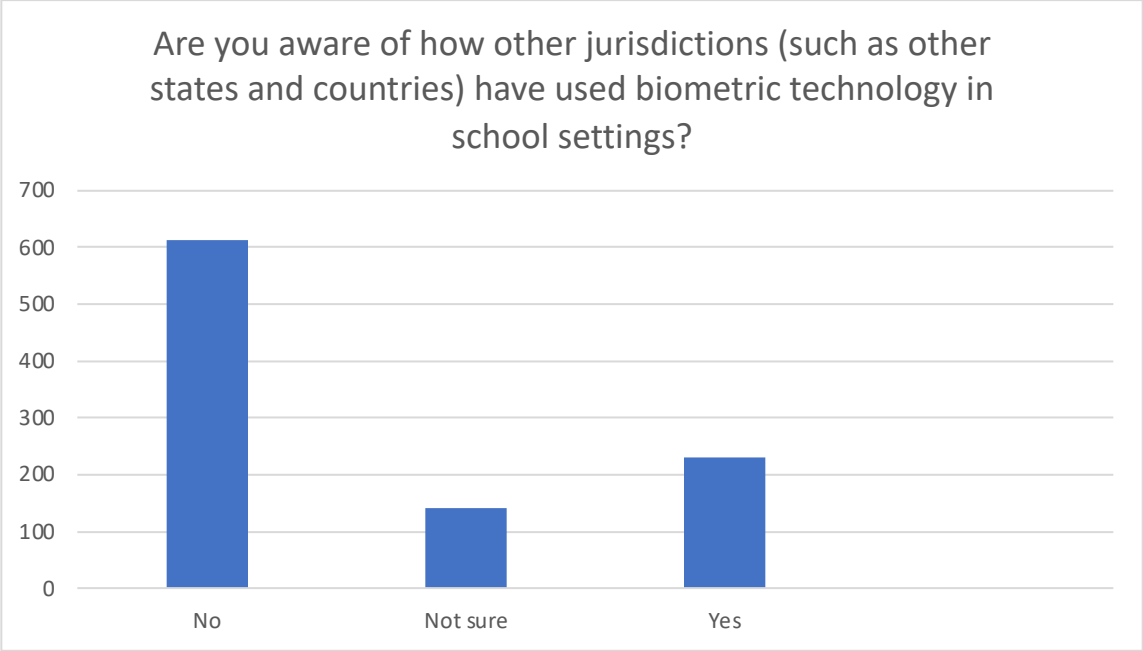
- Bathrooms and nurses' offices.
- Anything involving law enforcement use of the data.
- Tracking.
- In the classroom.
- Entry into the building.
- When parents do not consent.
- In any situation where the student can't opt out.
- Logging into devices
- All situations.
- On students generally.
- General surveillance.

Why should biometric technology NOT be used regardless of the situation? (Most frequent responses)

- Little need for it.
- Privacy issues.
- Risks outweigh the benefits.
- Lack of accuracy for FRT.
- Invasiveness.
- Poor investment.
- Data breach.

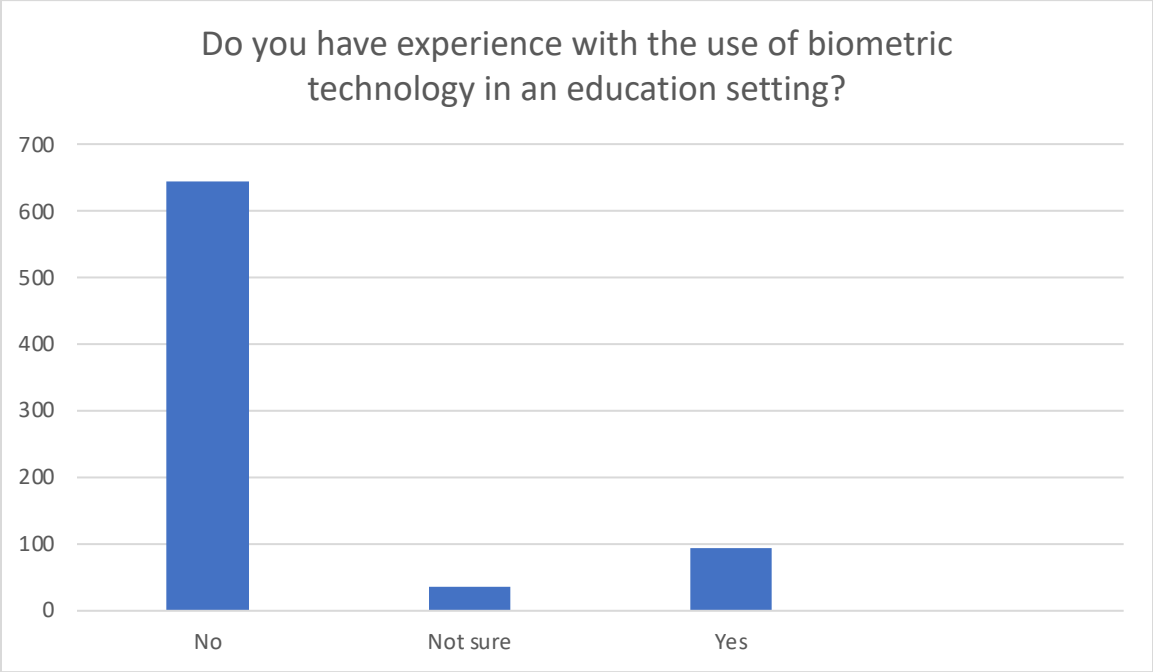

Are there any conditions or requirements that you feel could make the use of such technology appropriate?
700
600
500
400
300
200
100
0
No
Not sure
Yes


Would your response change if the use was limited to access to a device that is used for instructional purposes and the biometrics are stored on the device?
100
90
80
70
60
50
40
30
20
10
0
No
Not sure
Yes



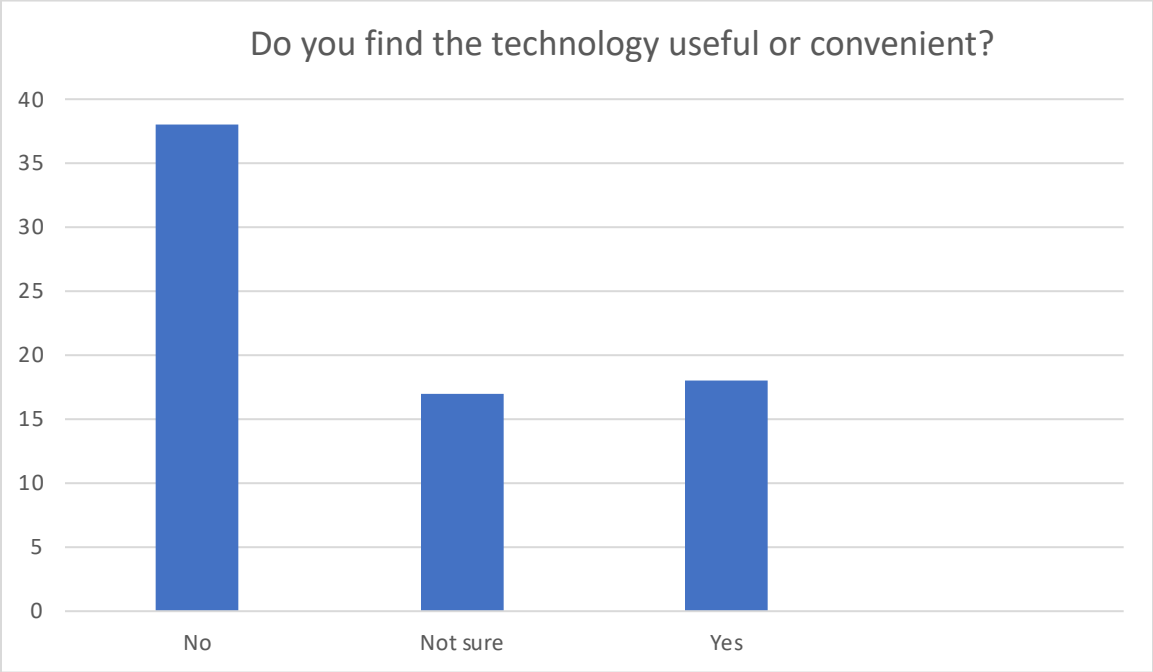
What are your thoughts on the usage of biometric technology in school settings in other jurisdictions (such as other states and countries)? (Most frequent responses)

- Inappropriate in the school setting.
- Invasion of privacy.
- Inappropriate for children.
- Causes harm.
- Waste of funding.
- Colleges use it successfully.
- Improves safety.
- Unconstitutional.



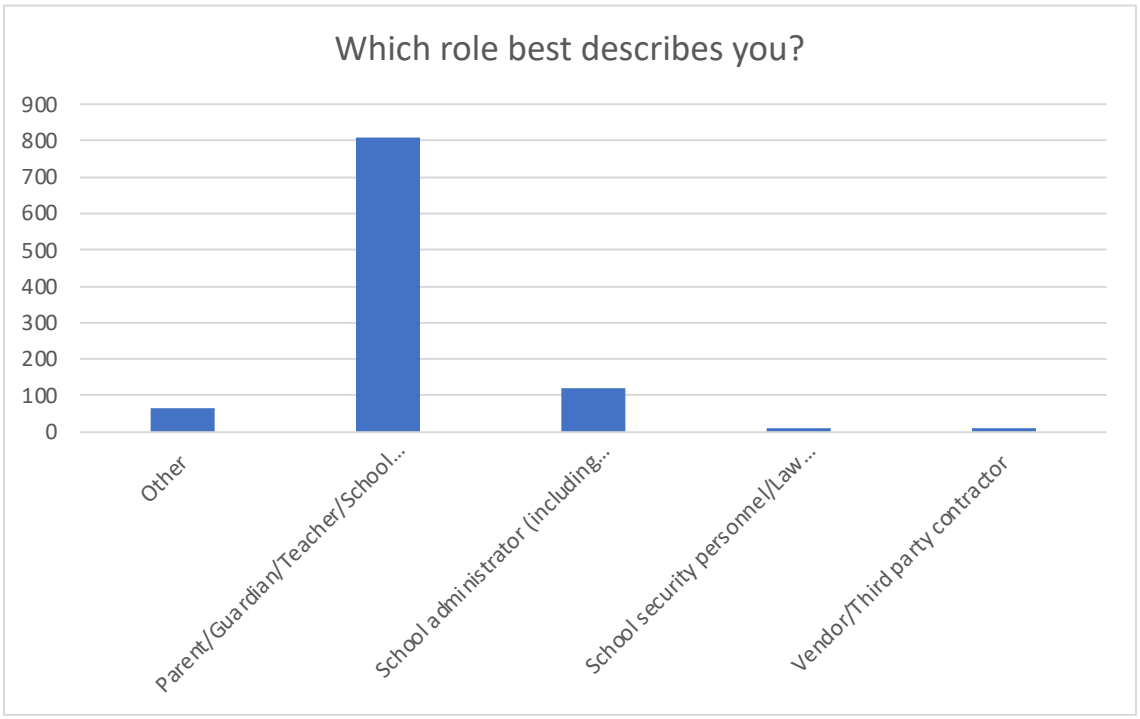
Please provide a detailed description, including the type of technology, the use, the duration of your experience with it and how often you used it.

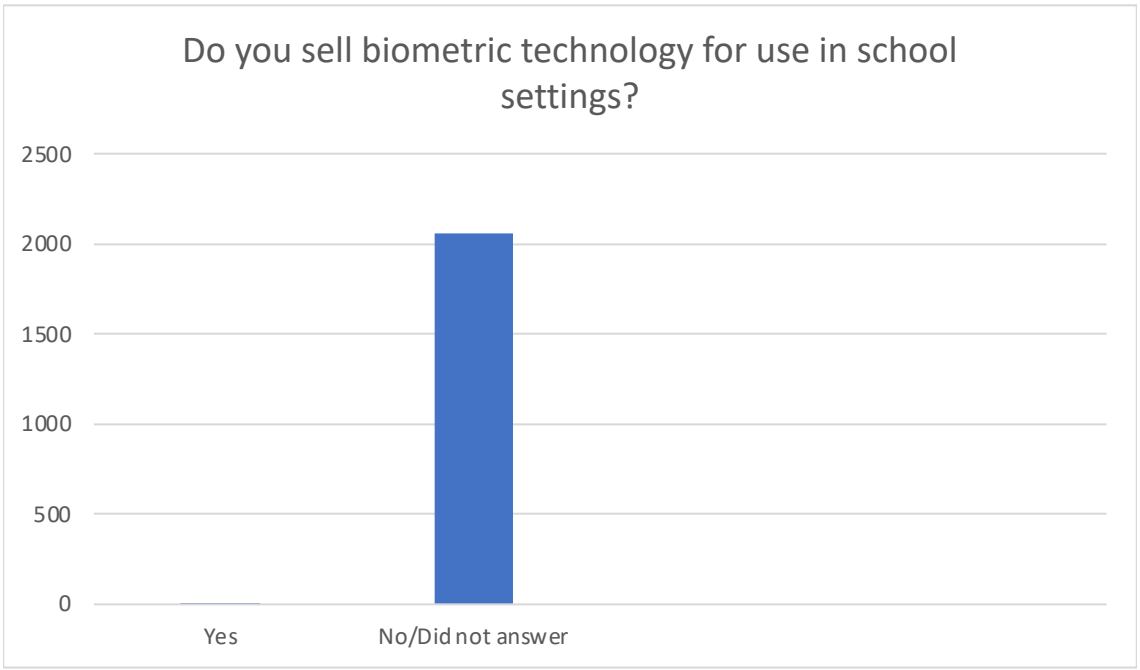
- Fingerprint scanning for lunch payments.
- Facial recognition generally.
- Fingerprints for logging into computers.
- Piloting facial recognition.
- Palm print to enter the library.
- Face ID to unlock devices.
- Staff clocking in and out with fingerprint.
- Voice to text for students with disabilities.



How or why is this technology useful or convenient? (Most frequent responses)

- To prevent school shootings.
- To keep unauthorized persons out of the school.
- Adds to overall security of school.
- Saves time.
- Ease of access.
- Can be helpful for children with learning disabilities.


Which role best describes you?
900
800
700
600
500
400
300
200
100
0
Other
Parent/Guardian/Teacher/School...
School administrator (including...
School security personnel/Law...
Vendor/Third party contractor


Do you sell biometric technology for use in school settings?
2500
2000
1500
1000
500
0
Yes
No/Did not answer

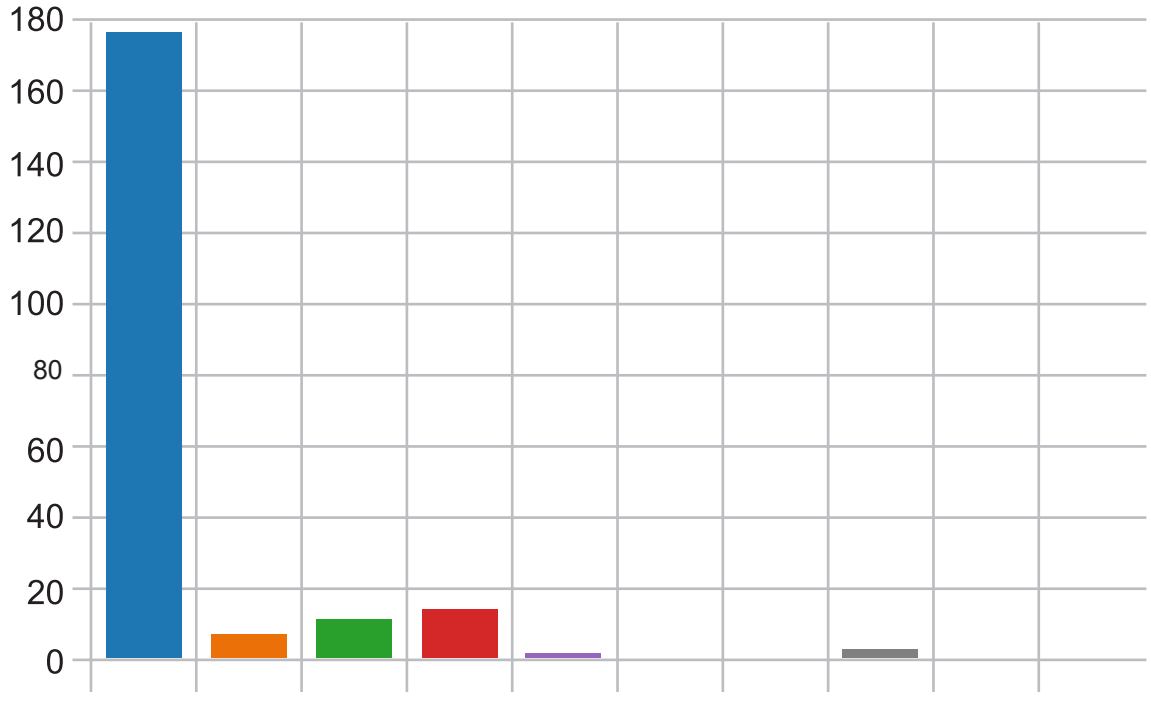
SED Educational Use of Biometrics Study:

Exhibit B

Educational Agency Use of Biometrics Study

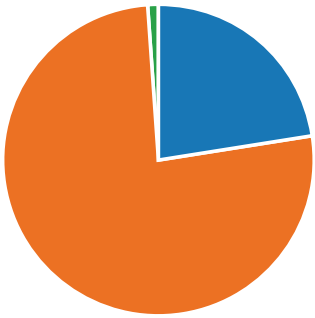
1. Please select your type of Educational Agency

School District/School	177
853 School	7
BOCES/RIC	11
Charter School	14
Non-public private or religious school	1
4410 School	0
State Supported School	0
Special Act School District	2
UPK Program other than a 4410 School	0
Other Type of Educational Agency Not Listed	0



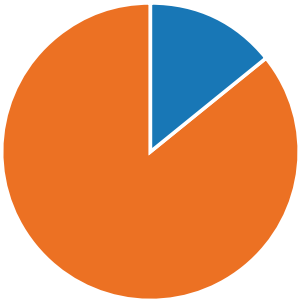
2. Does or did your Educational Agency use any biometric identification technology?

Yes	48
No	162
Unsure	2



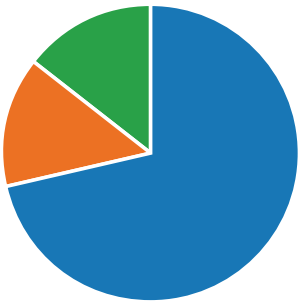
3. Has your Educational Agency used facial recognition technology?

Yes	7
No	42
Unsure	0



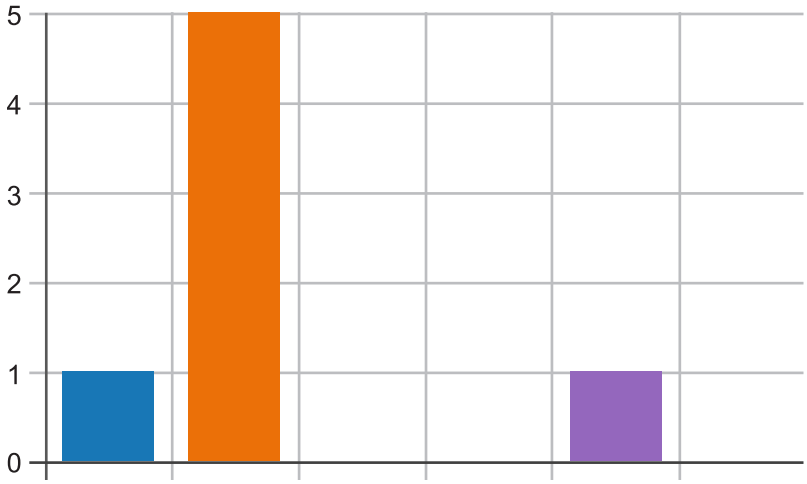
4. Does or did the facial recognition technology match images one-to-one (verification) or perform one-to-many matching (identification)?

Verification (one-to-one matching)	5
Identification (one-to-many matching)	1
Not sure	1



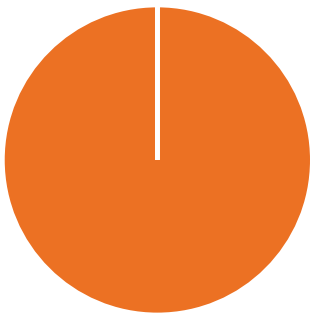
5. On whom is or was the facial recognition technology used?

Students Only	1
Teachers and Staff Only	5
Students, Teachers and Staff	0
All adults	0
Everyone who enters the building	1
Not Sure	0



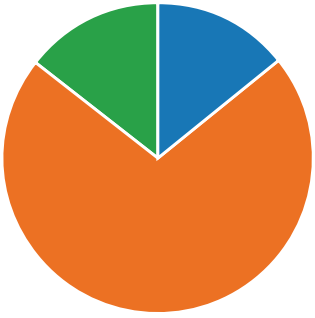
6. Does or did the facial recognition system use student photos for determining students' identities?

Yes	0
No	2
Uncertain	0



7. Does or did the software also provide weapon recognition?

Yes	1
No	5
Unsure	1

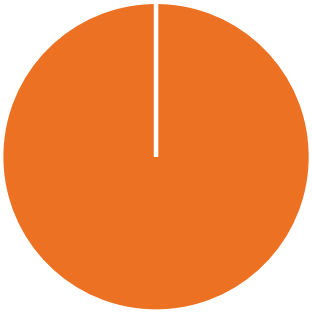


8. Please select which purposes your Educational Agency uses or used facial recognition technology (answer may be more than one).

School Security Screening	0
School Security - Other	1
Device Security (Such as Apple FaceID)	5
Other	3

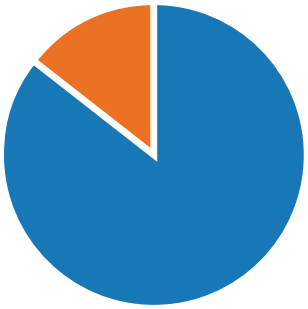
9. Is or was your Educational Agency's facial recognition technology connected to law enforcement?

Yes	0
No	7
Do not know.	0



10. Has your Educational Agency used biometric technology, other than facial recognition?

Yes	42
No	7



11. Please select the Educational Agency's uses of other biometric identification technology, other than facial recognition.

Touch ID access to a room, locker or other area	0
Touch ID to purchase items in the cafeteria for from a vending machine	7
Touch ID to access a technological device, including tablets	0
Other	29

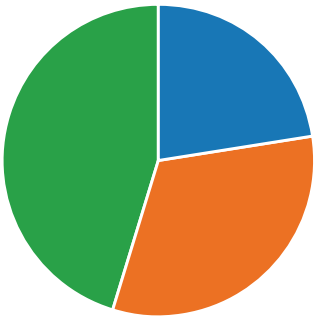
12. Please describe how your Educational Agency uses this technology, if not described above.

29
Responses

Latest Responses
"Touch ID to clock in and out"

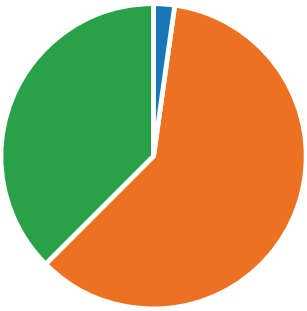
13. Is your Educational Agency considering the use of biometric technology in the future, if legally allowed?

Yes	48
No	68
Unsure	95



14. Have parents, students or advocates objected to your Educational Agency's use or proposed use of biometric technology?

Yes	6
No	126
Unsure	78



15. If you answered yes to the question regarding objections to the use or proposed use of biometric technology, please describe the objections.

6
Responses

Latest Responses
"Parents are concerned about privacy."

16. In the future, would your Educational Agency consider using facial recognition technology for school security and safety purposes?

Yes	46
No	51
Maybe	113

17. Please select the reason(s) why you would consider facial recognition technology for school safety and security.

Facial recognition systems can also detect weapons	61
Provide an alert when a person with a history of violence is entering	108
Have a video record of people who have entered school property	103
It is a deterrent for those who may wish to bring a weapon onto school property	69
Other	27

18. Would a representative from your educational agency be willing to assist the State with its study on the use of biometric identifying technology in schools, which study is required by State Technology Law section 106-b? NYSED and ITS seek feedback from educational agencies that use these technologies, particularly facial recognition. Any assistance and feedback would be greatly appreciated.

Yes	71
No	139

Acknowledgements

ITS wishes to thank the following groups and individuals who provided their insight, expertise, or knowledge for this report:

- The Advanced Information Security and Privacy (AISP) Research Lab at SUNY Canton
- Dr. Kambiz Ghazinour, Associate Professor, Center for Criminal Justice, Intelligence and Cybersecurity and Director of the AISP Lab, SUNY Canton
- Spencer Lawrence, SUNY Canton
- Antony Haynes, Esq., Associate Dean for Strategic Initiatives, Director of Cybersecurity and Privacy Law, and Associate Professor of Law, Albany Law School
- Jason Thomas, Albany Law School
- Anna Gabalski, Albany Law School
- Parents, students, teachers, administrators, security professionals, advocates, and all other groups and individuals that responded to the ITS Survey on the Use of Biometric Technology in Education, participated in the public meeting in 2022, or otherwise provided their comments and feedback on this topic

Office of Information Technology Services